



America at Risk: Closing the Security Gap



FEBRUARY 2004



PREPARED BY THE DEMOCRATIC MEMBERS OF THE
HOUSE SELECT COMMITTEE ON HOMELAND SECURITY

JIM TURNER, RANKING MEMBER

America at Risk:

Closing the Security Gap

Prepared by the Democratic Members of the
House Select Committee on Homeland Security
Jim Turner, Ranking Member

228 Adams Building
101 Independence Avenue, SE
Washington, DC 20540
202-226-2616
<http://www.house.gov/hsc/democrats/>

**DEMOCRATIC MEMBERS OF
THE HOUSE SELECT COMMITTEE ON HOMELAND SECURITY**

Jim Turner, Texas

Ranking Member

Bennie G. Thompson, Mississippi

Ranking Member, Subcommittee on Emergency Preparedness and Response

Loretta T. Sanchez, California

Ranking Member, Subcommittee on Infrastructure and Border Security

Louise M. Slaughter, New York

Ranking Member, Subcommittee on Rules

Zoe Lofgren, California

Ranking Member, Subcommittee on Cybersecurity, Science, and Research & Development

Karen McCarthy, Missouri

Ranking Member, Subcommittee on Intelligence and Counterterrorism

Edward J. Markey, Massachusetts

Norman D. Dicks, Washington

Barney Frank, Massachusetts

Jane Harman, California

Benjamin L. Cardin, Maryland

Peter A. DeFazio, Oregon

Nita M. Lowey, New York

Robert E. Andrews, New Jersey

Eleanor Holmes Norton, District of Columbia

Sheila Jackson-Lee, Texas

Bill Pascrell, Jr., New Jersey

Donna M. Christensen, U.S. Virgin Islands

Bob Etheridge, North Carolina

Ken Lucas, Kentucky

James R. Langevin, Rhode Island

Kendrick B. Meek, Florida

**Select Committee on Homeland Security
Democratic Staff**

David H. Schanzer
Staff Director & Chief Counsel

Mark T. Magee
Deputy Staff Director

John F. Sopko
General Counsel & Chief of Investigations

Scott D. Bates
Senior Policy Advisor

S. Camille Camacho
Executive Director

Moira Whelan
Press Secretary

Professional Staff Members

Carla D. Buckner
Peter Cleveland
Glenn Davis
Michael J. Eichberg
David Grannis
Gwendolyn M. Hall
Jessica R. Herrera
Jim McGee
Jason R. McNamara
I. Joshua Magarik
Daniel B. Prieto
Sue Ramanathan
Allen L. Thompson

With appreciation to the employees of the
Department of Homeland Security,
who are on the front lines, every day, working hard to protect
America.



Table of Contents

~

America at Risk: Introduction.....	i
Executive Summary.....	iv
 PREVENTING TERRORIST ATTACKS	
Preventing Attacks by Improving Intelligence.....	1
Preventing Attacks by Securing Nuclear Material.....	12
Preventing Attacks through Biodefense & Preparedness.....	20
 PROTECTING OUR BORDERS ON SEA, LAND, & AIR	
Securing Our Ports.....	35
Securing Our Borders.....	46
Securing Our Skies.....	59
 PROVIDING SECURITY INSIDE AMERICA	
Protecting America's Critical Infrastructure.....	71
Protecting Chemical Plants.....	82
Protecting Cyberspace.....	87
Protecting the Food Supply.....	97
Protecting America with Information Technology.....	104
 PREPARING OUR COMMUNITIES	
Preparing Our Nation's First Responders.....	114
 PRESERVING OUR VALUES	
Reinforcing Security, Privacy, and Civil Liberties.....	125

America at Risk: Closing the Security Gap

Introduction

No responsibility of the Congress is more important to the security of our nation than the exercise of vigorous and thorough oversight of the new Department of Homeland Security. Implementing the largest reorganization of the federal government in almost forty years would be daunting enough. Given the urgency, however, to prevent, deter and respond to terrorist attacks – and knowing failure is not an option – the Administration, the new Department and its congressional overseers face a challenge unlike any in our history.

A lack of leadership or focus, or errors in prioritization or judgment can place the lives of thousands of Americans at greater risk. Poor management can result in the waste of taxpayer dollars, as multi-billion dollar contracts are awarded under pressure to get the job done.

America at Risk: Closing the Security Gap is the product of our commitment to steadfastly pursue our duty of congressional oversight on this first anniversary of the formation of the new department. We have relied upon our own independent investigations and research, as well as a broad range of respected expert opinion. This report highlights significant security gaps that still remain and offers recommendations to close those gaps that threaten the security of every American.

One year ago, on March 1, 2003, the Department of Homeland Security was formally established to protect the American people, the American economy, and, ultimately, American society from a terrorist attack. The origins of the Department trace back to the tragedy of September 11, 2001. On that day, as we absorbed the full horror of what had been done to us, we vowed that we would never again allow our defenses to be circumvented so easily.

In the wake of the attacks, the Congress united to act with unprecedented unity and speed. The Administration was authorized to take a variety of actions to protect us from terrorists, including the use of military force against al-Qaeda and the Taliban. In the months following September 11, legislation was enacted to bolster security at our seaports and airports, fortify our borders, and provide our intelligence and law enforcement communities with the tools needed to root out terrorists here and abroad. We worked together to create the Department of Homeland Security.

We are safer today than we were before the attacks of September 11, but the critical question is – are we as safe as we need to be?

It remains an uncomfortable but unassailable fact: America is not as safe as it needs to be in the face of the threat we face from those that seek to do us harm. Critical gaps in our homeland security continue to exist while al-Qaeda and like-minded groups continue to seek ways to kill our citizens, destroy property and infrastructure, disrupt our economy, and demoralize our nation. Our enemies are opportunistic, and will remain fixated on identifying and exploiting our weaknesses. We must remain vigilant in bolstering our homeland defenses as rapidly and effectively as we can to protect ourselves from any possible terrorist attack. As we move forward to strengthen our security we must be mindful that properly made, homeland security-related investments also offer substantial benefits in such critical areas as public health, crime prevention, technology development, the free flow of commerce, and all-hazards preparedness.

The men and women who patrol our borders, inspect cargo at our ports, analyze intelligence, and respond to emergencies, are setting the standard for excellence, but they must have the leadership and support they deserve. On this first anniversary of the Department of Homeland Security, our national homeland security efforts do not reflect the sense of urgency required in light of our enemy's declared intent to carry out an even greater event than occurred on September 11, 2001.

To protect the homeland, we must be alert in identifying our security gaps, inventive in determining the most effective ways to overcome them, and diligent in ensuring that such gaps never exist again.

We are mindful that efforts to date to secure the homeland have resulted in billions of dollars in new federal, state, and local expenditures. Any investment must be analyzed in terms of costs and benefits. While post-September 11 expenditures at the federal level are significant, some perspective is needed. For example, since September 11, we have increased annual discretionary spending for the agencies that now make up the Department of Homeland Security by upwards of \$15 billion. During the same period, we have increased our defense budget by upwards of \$135 billion. For fiscal year 2005, the Administration seeks an increase of about \$4 billion in total spending for the Department – an amount equal to one month's cost of the war in Iraq. We must succeed in achieving stability in Iraq. But in the broader War on Terror, we must commit whatever is necessary to protect the homeland. The cost of failure would far exceed any investment we make.

Our vision for homeland security includes a commitment to aggressively target terrorists wherever they may hide and invest in policies that will, over the longer term, prevent the rise of future terrorists. We are engaged not only in a conflict of will but a conflict of ideals, religion, history, and culture that stirs the irrational violence we know as “terrorism.” Throughout our history, Americans have met and overcome great challenges through firm resolve and sacrifice. America continues to offer the world’s best hope and promise of freedom and prosperity for all people.

In this report, we identify significant security gaps and propose ways to close them, not for the purpose of casting blame, but to make America stronger. We call on the Administration and our colleagues in Congress to take swift action on these recommendations to close the security gaps we now face. Our nation deserves nothing less.

Representative Jim Turner, (D-TX)

Ranking Member

U.S. House Select Committee on Homeland Security

EXECUTIVE SUMMARY

One year after the creation of the Department of Homeland Security (DHS), dangerous security gaps remain that place America at risk to the threat of terrorist attack. While we are safer today than we were before the September 11 attacks on our homeland, we are not as safe as we need to be to protect the American people from the threat of al Qaeda and like minded groups.

Our nation remains vulnerable to potentially catastrophic attacks involving nuclear, biological, chemical and radiological weapons. Pathways to the United States by land, sea and air are insecure. Our critical infrastructures have few defenses and our communities are not as prepared as they need to be to respond to a terrorist attack. We need to take faster and stronger action to close these security gaps. As the President has stated, we are at war, and therefore we must recapture the sense of urgency that existed in America two and a half years ago to protect our homeland.

We present this report in fulfillment of our constitutional obligation to vigorously oversee the Administration's homeland security efforts and our moral duty to recommend ways to make America safer. Summaries of many of the security gaps we have identified and our recommended solutions appear below. Some of the topics coincide with initiatives recently announced by the Department. We welcome these measures and will continue to work with the Administration and our colleagues in Congress to close the security gaps we face as soon as possible.

PREVENTING TERRORIST ATTACKS

Preventing Attacks by Improving Intelligence

Security Gaps:

- The DHS has still not completed a comprehensive threat and vulnerability assessment to set priorities and guide our strategy.
- The federal government has failed to develop a unified terrorist watch list accessible to border security personnel, state and local law enforcement, and others with homeland security responsibilities.
- The DHS's intelligence unit is still not functioning as intended; it is operating at less than 45 percent of its full strength.

Security Recommendations:

- The DHS should complete a comprehensive threat and vulnerability assessment as soon as possible, but no later than October 1, 2004.

- The Administration should exert the leadership necessary to complete a unified terrorist watch list as soon as possible.
- The DHS should complete its authorized hires of intelligence personnel so that the Information Analysis and Infrastructure Protection Directorate will be fully staffed and operational by October 1, 2004.

Preventing Attacks by Securing Nuclear Material

Security Gaps:

- Nuclear weapons and materials within the former Soviet Union and around the world are not secure and represent a direct threat to the United States.
- More than a dozen years after the break up of the Soviet Union, there are 105 nuclear sites within Russia and the former Soviet Union that need security improvements. They contain approximately 600 metric tons of nuclear materials, enough for about 41,000 nuclear warheads.
- Outside Russia, some twenty tons of highly enriched uranium exists at 130 civilian research facilities in 40 countries, many of which have no more security than a night watchman and a chain link fence.
- Domestic and international sources of radiological materials that can be used for a “dirty bomb” are also not secure. Federal investigators have documented 1300 cases in which radioactive material inside the U.S. have been lost, stolen, or abandoned over the past five years.

Security Recommendations:

- The Administration should follow the recommendations of the bipartisan Baker-Cutler Commission and triple resources dedicated primarily to securing nuclear materials and sites within the former Soviet Union.
- The United States should lead a global coalition to remove all vulnerable nuclear materials located outside the former Soviet Union and the Administration should increase its contribution to the Global Partnership Against the Spread of Materials of Mass Destruction.
- The Administration should identify vulnerable sources of radiological materials that could be used for a “dirty bomb” and takes steps to secure them. Licensing requirements should be tightened by ensuring that applicants are inspected before they may receive shipments of dangerous materials.

Preventing Attacks through Biodefense & Preparedness

Security Gaps:

- Dangerous stockpiles of biological agents developed by the former Soviet Union, as well as the human expertise built up in this, the largest and most intensive biological weapons program in history, are susceptible to theft or appropriation by terrorist groups. Security projects are underway at only four of 49 known biological sites with only two sites fully secured.
- Many U.S. facilities handling deadly pathogens have not had their security, inventories, and personnel reviewed, registered and certified by the government as required by law. The Administration missed (and then extended indefinitely) its own November, 2003 deadline for completing this review.
- Today, at least 57 different countermeasures are needed to defend against 19 of the major bioterrorist agents. Currently, only one of these countermeasures can be widely distributed. No vaccine is available for botulinum toxin, bubonic plague or tularemia. Virtually nothing has been done to address the growing threat presented by bioengineered pathogens.
- One year after the creation of DHS, there is still no comprehensive Biodefense Preparedness and Response Plan. Our public health infrastructure is poorly equipped to both detect and respond to a biological attack. Only six states have enough laboratory capacity to deal with a public health emergency and only two have sufficient workers to distribute vaccines in response to a biological attack. The National Smallpox Vaccination program has failed: it targeted the vaccination of 500,000 emergency workers and ten million first responders, only 39,000 have been vaccinated.

Security Recommendations:

- Efforts to secure weapons of mass destruction stockpiles around the globe should be tripled, consistent with the recommendations of the bipartisan Baker-Culter Commission and a portion of those funds should be dedicated toward securing biological stockpiles from the former Soviet Union.
- The Administration should make it a high priority to implement fully the legally mandated program to secure biological pathogen stocks in the United States.
- To develop the medicines and vaccines necessary to protect us, and the rest of the world, from bioterrorism, the United States should move beyond the limited confines of the Administration's "Project Bioshield" by developing robust, effective public-private partnerships for the development of new diagnostics, drugs, and vaccines. We must also move forward with the speed and resources reminiscent of the

Manhattan Project, in an effort to reduce the time necessary to move from “bug to drug” (pathogen detection to drug response) from years to a matter of weeks.

- The Administration should work in conjunction with state and local officials, health care providers, researchers and the private sector to develop a comprehensive Biodefense Strategy focusing on prevention, preparedness and response. This plan, which is long overdue, should be completed as soon as possible.

SECURING AMERICA BY SEA, LAND, AND AIR

Securing Our Ports

Security Gaps:

- The seven million cargo containers that arrive at American ports and move through our communities by truck and rail, only a small percentage of which are physically inspected or mechanically screened, represent a severe security threat as they are possible delivery devices for weapons of mass destruction.
- The vast majority of cargo containers that travel to and through the U.S. have no tamper resistant seals. The Administration has not established security standards for container seals.
- Millions of cargo containers are entering America without having been screened for radiological or nuclear devices.
- There are less than 100 inspectors currently assigned to foreign ports under the Container Security Initiative to screen the seven million cargo containers before they come to our shores. These inspection teams are unable to review all the manifests of cargo shipments headed toward the U.S.
- Of the 5,300 companies whose shipments receive reduced scrutiny at seaports due to their membership in the Customs-Trade Partnership Against Terrorism program (C-TPAT), only 130 have been audited and verified as meeting the program’s security requirements.
- The Coast Guard has estimated that ports need to spend \$1.1 billion this year, and \$5.4 billion over ten years, to meet security standards set by the Coast Guard as instructed by Congress. The Administration’s budgets since 9/11 have requested only \$46 million for port security and although Congress has provided much more funding, there remains a \$566 million funding gap for this year alone.

Security Recommendations:

- Radiation detection portals and other non-intrusive inspection technologies should be deployed in sufficient numbers to screen every cargo container entering America's ports and be integrated into normal port operations so they do not slow the flow of commerce.
- The DHS should require containers entering the U.S. to have a high security seal that meets international standards.
- The DHS should deploy robust inspection teams to the largest ports abroad and ports in high risk countries. Inspectors should be deployed for at least one year.
- All the companies in the C-TPAT program should be inspected by DHS to ensure that they meet minimum security requirements.
- Additional federal assistance is needed to meet short term security needs at America's ports this year. In the future, the federal government, ports, and industry should share the cost of providing robust port security.

Securing Our Borders

Security Gaps:

- There is only one border patrol for every 5.5 miles of our northern border. The Administration met its legal requirement to triple the number of border patrols on the northern border by moving hundreds of employees from the southern border. Staffing levels for border patrol, and customs and immigration inspectors are far below levels set by Congress and the Administration has not developed a new border staffing strategy for either the northern or southern border since September 11.
- Underinvestment in infrastructure impedes security programs, slows the flow of commerce and burdens the economies of border communities. A total of 64 land ports of entry have less than 25 percent of the required inspection space.
- Trucks entering the U.S. on the southern border are not comprehensively screened for nuclear or radiological materials. Tamper resistant seals are required on trucks crossing the southern border, but not the northern border.
- Citizens of 27 "visa waiver" countries are currently exempt from coverage of the US-VISIT system. Thus, people like the "shoe bomber" Richard Reed (a British national) and the alleged al Qaeda operative Zacarias Moussaoui (a French national) would not be fingerprinted and photographed under the US-VISIT system.

- Border security systems like US-VISIT are not currently linked to a comprehensive terrorist watch list.

Security Recommendations:

- The Administration should immediately develop and implement a comprehensive post-9/11 national border strategy that will allow DHS to effectively deploy its personnel and technology.
- The Administration should take advantage of this historic opportunity to revitalize our borders by investing in roads, other infrastructure, and inspection facilities that will allow for implementation of needed security programs while facilitating the legitimate travel and trade. The Administration should consider the full impact of US-VISIT on border communities and incorporate community representatives in the US-VISIT planning process.
- Radiation portal monitors should be installed immediately at all border crossings to support 100 percent screening of truck cargo for nuclear and radiological materials.
- Border security programs like US-VISIT should be linked to a comprehensive terrorist watch list as soon as it is completed so that border security personnel have real-time access to the most current watch list information available.

Securing Our Skies

Security Gaps:

- Despite massive expenditures, Transportation Security Administration (TSA) airport screeners continue to allow dangerous items to enter U.S. passenger planes.
- Most air cargo shipped on passenger planes is not screened for explosives. TSA does not audit the security practices of all the companies (“known shippers”) permitted to place cargo on passenger aircraft.
- Passenger airliners have no defenses for surface to air missiles.
- Cargo aircraft that fly over the United States are not required to have hardened cockpit doors.
- Many airport employees are permitted to access sensitive areas of the airports without going through routine passenger screening.

Security Recommendations:

- The TSA should determine how many screeners should be deployed to ensure security and, if necessary, the artificial cap of 45,000 screeners should be lifted. TSA should provide more rigorous screener training and more frequent tests of the screening process.
- TSA should provide greater security for air cargo on passenger aircraft, with the goal of 100 percent inspection as soon as possible. The security practices of all “known shippers” should be verified.
- The DHS should develop and deploy as soon as feasible, technology that can protect passenger airliners from attack by shoulder fired missiles.
- Cargo flights passing over the United States should be required to have hardened cockpit doors.
- All persons who enter areas beyond the screening checkpoint should be screened for dangerous items.

PROVIDING SECURITY INSIDE AMERICA
--

Protecting America’s Critical Infrastructure**Security Gaps:**

- America’s chemical facilities, food supply, water systems, telecommunications facilities, electrical grid, energy plants, pipelines, roads, bridges, tunnels, dams, subways systems, hospitals, skyscrapers and arenas are all potential targets for terrorist attacks – yet the Administration has not taken strong action to secure even the most vulnerable and dangerous of these critical infrastructures, relying too heavily on voluntary private action.
- The Administration has not completed a comprehensive risk assessment to identify our greatest vulnerabilities and prioritize implementation of protective measures. One senior DHS official estimated that completion of such a study would take five years.

Security Recommendations:

- The Administration should explore tax and other incentives to increase infrastructure security, speed the development of commercial products like terrorism insurance, and as necessary, develop a minimum regulatory framework that does not place

unreasonable demands on business owners, such as requirements to undergo periodic vulnerability assessments and security audits.

- The Administration should complete, as soon as possible, but no later than October 1, 2004, an initial national critical infrastructure risk assessment. The recent announcement that DHS will create a national database of critical infrastructure is but the first step toward the development of a genuine infrastructure risk assessment.
- The Administration should establish an annual, sector-by-sector report card and awards program recognizing significant improvements or achievements in critical infrastructure protection.

Protecting Chemical Plants

Security Gaps:

- Today there are 123 chemical facilities in the U.S. that could threaten over one million people in the event of a massive breach of chemical containment due to a terrorist attack.
- Unlocked gates, absent guards, dilapidated fences and unprotected tanks filled with deadly chemicals occur at dozens of plants across the country.

Security Recommendations:

- The Administration should require all facilities that pose a substantial danger to conduct vulnerability assessments, develop security plans to address vulnerabilities and submit these plans to DHS by October 1, 2004.

Protecting Cyberspace

Security Gaps:

- There is no senior level official in the Administration who has the explicit authority to direct the multiple agencies necessary to prevent and respond to a cyber-9/11. There is no central organization through which officials from the federal government and private industry can coordinate and respond to a cyber-crisis.
- Government computer networks are insecure. Eight of the agencies surveyed received failing grades on their cybersecurity from the House Government Reform Committee. The DHS received the lowest score: 34 of 100.

- Home computer systems are also vulnerable and can be used as launching points for “distributed denial of service” and other attacks. These attacks are causing billions in damages.

Security Recommendations:

- A new senior level official for cybersecurity should be designated who will report directly to either Secretary Ridge or the President.
- The Administration should create a National Crisis Coordination Center that could house, within a single facility, representatives from the private sector, federal, state and local government agencies who can bring relevant parties together in the event of a cyber-9/11.
- All government agencies should require that the software they purchase is preconfigured with the highest level security settings.
- A Chief Security Officer should be appointed in the Office of Management and Budget to coordinate the federal government’s efforts to secure its computer systems.
- The federal government and the private sector should establish a framework specifying the actions that each should take to help individual computer users to secure their systems.

Protecting the Food Supply

Security Gaps:

- The FDA currently inspects only two percent of food imports under its jurisdiction. USDA’s one percent increase in inspectors at food facilities is insufficient in light of the severity of the threat.
- Lab testing capacity necessary to rapidly detect threats to agriculture and food does not exist in every state.
- The Administration does not yet have a national response plan for preparing and defending the nation against catastrophic attacks on our agricultural system or food supply.

Security Recommendations:

- USDA, FDA, and DHS should deploy additional food inspectors to our borders and food processing and packing plants.

- At least one lab in every state should have the capability to conduct tests for key agro-terror threats.
- The DHS should take the lead in developing a comprehensive national agro-terrorism response plan within the next year that contains specific goals and timetables for achieving those goals.

Protecting America with Information Technology

Security Gaps:

- By merging 22 agencies together, DHS inherited as many as 8,000 information technology applications, one hundred of which are considered “major.” Yet, DHS has not harmonized basic systems to manage the department, like accounting, procurement, grant management, and budgeting. In many instances, benefits and payroll continue to be provided by legacy agencies. According to a DHS senior official, DHS keeps a “running hand-tallied list of its staff, with the total varying from 190,000 to 225,000 depending on which of the 22 component agencies’ 24 human resources systems are consulted.”
- The Administration is not taking advantage of information technology for homeland security needs in key areas such as information sharing across agencies and with state and local governments. The Markle Foundation concluded that “the government’s progress toward building an adequate network has been slow and is not guided by an overall vision.”

Security Recommendations:

- The Administration should make extensive use of the most up-to-date information technologies to improve homeland security functions and unify DHS into a more cohesive organization. The DHS should establish clear milestones and timelines for completing its major information technology initiatives.
- Management and procurement of information technology need to be strengthened by increasing the authority of the Chief Information Office and Chief Procurement Officer.
- The DHS should create an information technology “red team,” which includes leading private sector experts, to advise the Department on how to speed integration of its information technology infrastructure and plug critical gaps in current systems.

PREPARING OUR COMMUNITIES

Preparing Our Nation's First Responders

Security Gaps:

- Two and a half years after the attacks of September 11th, many first responders still lack interoperable communications equipment and cannot communicate with one another. The Administration has allocated no new funds in its proposed fiscal year 2005 budget to address the issue.
- The DHS has still not established a set of essential capabilities that all communities should have, based on the threats and vulnerabilities they face, to respond to terrorist attacks. Despite the expenditure of billions of dollars, we have no way to measure how and whether we are adequately preparing to protect communities throughout America.
- Federal grant programs are not getting money to our communities quickly enough. Distribution of funding is based on arbitrary formulas rather than the risks that communities face – California, New York, Texas and Florida received about \$6 per capita while states like Wyoming, North Dakota, and Vermont received over \$30 per person.

Security Recommendations:

- Technologies that provide short-term, baseline communications already have been identified by state and local officials. The DHS's recent announcement that it will provide "technical specifications" for these systems is nothing new. Rather than re-identifying these technologies, DHS should provide a dedicated, annual funding source to assist communities in deploying affordable, existing technologies that would enable first responders to communicate at the scene of a disaster right now.
- The Department should determine the essential capabilities necessary for first responders to protect every community in America, and then make the commitment to obtain these capabilities and provide first responders with the tools they need to do their jobs.
- Grant programs should be consolidated and revised as proposed in bipartisan legislation before the Select Committee on Homeland Security. Funding should be based on an assessment of threats and vulnerabilities, not formulas.

PRESERVING OUR VALUES

Reinforcing Security, Privacy, and Civil Liberties

Security Gap:

- In the past year, homeland security initiatives, such as data mining efforts and an airline passenger screening system, have been derailed or postponed because the Administration has failed to adequately evaluate the programs' effects on privacy and civil liberties.

Security Recommendations:

- The Administration should create a Chief Privacy Officer responsible for evaluating privacy issues that arise in conjunction with the development and use of new technologies in the federal government. Congress should consider creating offices like the DHS Privacy Office in other agencies with substantial homeland security responsibilities.
- The Administration should create a Commission on Privacy, Freedom and Homeland Security to evaluate the implementation of homeland security initiatives in a way that reinforces our fundamental constitutional rights and values.

PREVENTING TERRORIST ATTACKS

Preventing Attacks by Improving Intelligence

Good intelligence used effectively is the key to preventing terrorist attacks. While the intelligence failures leading up to the September 11, 2001, attacks have been well documented, major shortcomings continue to frustrate intelligence efforts. New intelligence capabilities, such as a comprehensive and integrated terrorist watch list, are not yet in place, and old problems, such as insufficient sharing of terrorist threat intelligence, remain. To remedy these shortcomings, the Administration should clarify the mission of the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate, complete a comprehensive strategic threat and vulnerability assessment to prioritize protective measures and guide homeland security strategic planning, and improve the sharing of information among federal agencies, with state and local governments and with the private sector.

The bipartisan Congressional Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001 (Congressional Joint Inquiry) stated that the U.S. government was unable to prevent the al Qaeda attacks due to failures in collecting intelligence, assembling and analyzing the information that was collected, placing suspected terrorists on watch lists, understanding the terrorist threat as it related to specific U.S. security vulnerabilities, and sharing information across government agencies and with state and local authorities.¹

These failures suggest that defeating the threat of terrorism requires a new and different type of intelligence structure than was needed during the Cold War or for past military operations. The challenge now is to understand a terrorist threat that is decentralized, with small cells of operatives focused on attacking non-traditional targets such as airliners or other civilian infrastructure. Our government needs to be equally agile in "connecting the dots," and sharing information collected from disparate sources with those in place to prevent terrorist attacks.²

SECURITY GAP: The Directorate of Information Analysis and Infrastructure Protection Suffers From an Unclear Mission and Insufficient Resources.

Congress sought to address the intelligence failures of September 11, 2001 and provide an effective counterterrorism intelligence unit when it created the Department of Homeland Security

¹ House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, *Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001*, House Report 107-792 and Senate Report 107-351, December, 2002.

² See, for example, (a) Markle Foundation, *Protecting America's Freedom in the Information Age*, (New York: Markle Foundation, October, 2002); (b) James B. Steinberg, Mary Graham, and Andrew Eggers, "Building Intelligence to Fight Terrorism," *the Brookings Institution*, September 2003; (c) Kevin O'Connell and Robert R. Tomes, "Keeping the Information Edge," *Policy Review*, December 2003; and (d) Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. *Fifth Annual Report to the President and Congress*. (Arlington, VA: RAND, December 15, 2003).

(DHS) Directorate of Information Analysis and Infrastructure Protection (IAIP). Consistent with the 2002 Homeland Security Act, the IAIP Directorate is charged with analyzing intelligence related to the terrorist threat on the homeland; mapping the terrorist threat to specific vulnerabilities; conducting assessments of the terrorist threats and vulnerabilities in order to make appropriate recommendations for prioritizing security efforts according to threat; disseminating intelligence to federal, state, and local officials to improve prevention measures; and conducting threat alerts.³

Since the passage of the Homeland Security Act, however, the key task of assembling, analyzing, and assessing intelligence related to the terrorist threat on the homeland has been taken over by the Terrorist Threat Integration Center (TTIC). The President announced the creation of TTIC in January, 2003, during the State of the Union Address as the center for terrorist-related threat analysis and assessments.⁴ The TTIC is currently a “joint venture” between the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and DHS, with a director that reports to the Director of Central Intelligence. Additionally, consistent with the mandate of the Homeland Security Act, responsibility for operating a comprehensive government terrorist watch list previously had been assigned to DHS. However, the task of compiling and administering such a watch list has now been assumed by the Terrorist Screening Center (TSC), which is part of the FBI.⁵

Moreover, the FBI’s own Counter Terrorism Division has expanded dramatically since September 11, 2001, and it has assumed some of the responsibilities that Congress placed within DHS for intelligence analysis and information sharing.⁶ The Department of Defense’s newly created Northern Command also boasts an intelligence fusion center that analyzes and disseminates information on threats to the homeland.

The creation of TTIC and TSC and the expansion of intelligence functions within previously existing agencies has led to confusion about the central mission of the IAIP Directorate. While it still seeks to map terrorist threats against U.S. vulnerabilities and disseminate threat information to state and local officials, it is no longer in a position to act as the federal government’s central fusion center to receive and analyze all terrorist threat-related information as envisioned by the Homeland Security Act. It cannot serve as the main entity to “connect the dots,” as was called for in the aftermath of September 11, 2001, but must instead coexist with other intelligence agencies who have now assumed one of its key intended functions. According to the DHS Inspector General, the TTIC and TSC “either overlap with, duplicate, or even trump [the authorities] of IAIP. Ensuring that DHS has access to the intelligence that it needs to prevent and/or respond to

³ “Homeland Security Act of 2002.” (P.L. 107-296, §201).

⁴ The White House, “Strengthening Intelligence to Better Protect America,” February 14, 2003. <http://www.whitehouse.gov/news/releases/2003/02/20030214-1.html>.

⁵ The White House, “New Terrorist Screening Center Established,” September 16, 2003. <http://www.whitehouse.gov/news/releases/2003/09/20030916-8.html>.

⁶ According to House Report 108-401 accompanying the Omnibus Appropriations Act for fiscal year 2004, 523, “Since the terrorist attacks on September 11th, 2001, the FBI has shifted its main focus from investigating crimes to preventing acts of terrorism. Inherent in this transformation is a greater emphasis on collection, management, and analysis of data and intelligence, and greater collaboration across all levels of law enforcement. The urgency to prevent acts of terrorism has required the infusion of substantial resources, with the FBI growing by over 50 percent in just three years.”

terrorist threats is, under such circumstances, an even harder challenge than it would otherwise be.”⁷

Compounding the IAIP Directorate’s inability to carry out one of its central missions is its current shortage of resources. Although Congress approved funds for 692 employees for the Directorate for fiscal year 2004, fewer than 300 people had been hired as of February 11, 2004.⁸ This has translated into fewer personnel available to serve in liaison positions at other intelligence entities. For example, as of November 20, 2003, DHS had assigned only five full-time analysts to TTIC of the 30 to 45 projected to be necessary.⁹ Also, in a broader budget context, the President’s fiscal year 2005 budget proposes that DHS will no longer contribute any funding to TTIC and the TSC, as is currently being done.¹⁰ Given that budget authority can equate to influence in ensuring that it receives the intelligence information required to prevent and respond to terrorists threat, DHS, under such circumstances, potentially faces additional barriers to fulfilling its mission.

SECURITY RECOMMENDATION

The Administration should take steps to reinvigorate the IAIP Directorate in recognition of its central role in fulfilling a core function of the Department of Homeland Security. Specifically, it should clarify the mission of the Directorate in light of the creation of the TTIC and the TSC and the expansion of terrorist threat analysis functions of other government agencies and ensure that the Directorate has the full range of staffing, technological, and physical resources necessary to carry out its legally mandated duties. The Administration should propose amendments, if needed, to the Homeland Security Act to clarify IAIP’s missions and responsibilities. The Administration should also ensure that the IAIP Directorate receives access to all intelligence information it may require in carrying out its responsibilities under the Homeland Security Act, despite any future funding arrangements for the TTIC and TSC.

⁷ Department of Homeland Security, Office of Inspector General, “Major Management Challenges Facing the Department of Homeland Security,” December 31, 2003, 6.

<http://www.dhs.gov/interweb/assetlibrary/FY04managementchallenges.pdf>.

⁸ Briefing by IAIP staff for staff of the House Select Committee on Homeland Security, February 13, 2004. An additional 100 personnel are in the process of being hired by the Directorate. The President’s fiscal year 2005 request seeks no significant increase in personnel for the IAIP Directorate.

⁹ John O. Brennan, Director, Terrorist Threat Integration Center. December 4, 2003. Response to Questions for the Record, Joint hearing of the House Select Committee on Homeland Security and House Judiciary Committee, “The Terrorist Threat Integration Center and its relationship with the Departments of Justice and Homeland Security.” July 22, 2003.

¹⁰ According to Administration fiscal year 2005 budget request documents for the IAIP Directorate, “There is a \$19.3 million decrease from [fiscal year 2004] which [sic] reflects the Administration’s proposal to centrally fund the Terrorist Threat Integration Center (TTIC) with other intelligence programs and the Terrorist Screening Center (TSC) with Department of Justice programs. President’s Budget Request does not seek funding for TTIC and TSC within IAIP for FY 2005.” U.S. Department of Homeland Security, *Department of Homeland Security Information Analysis and Infrastructure Protection (IAIP) Fiscal Year 2005 Congressional Budget Justification*, (Washington: Department of Homeland Security, February 2, 2004), 23.

SECURITY GAP: We Lack a Threat and Vulnerability Assessment.

The Department of Homeland Security needs a comprehensive terrorist threat and vulnerability assessment to prioritize its actions to protect the homeland. According to Michele Flournoy of the Center for Strategic and International Studies:

Such an assessment is critical to setting priorities, reconciling competing interests, and allocating resources effectively.... Without a regular, disciplined, and comprehensive threat and vulnerability assessment process that considers both the probability of various types of attacks and the severity of their consequences, decision makers will have little analytic basis for making tough strategy choices about where to place emphasis, where to accept or manage a degree of risk, and how best to allocate resources to improve America's security.¹¹

While threats to critical infrastructure would account for much of this assessment, acts of terror directly against populations should also be included. The need for a comprehensive threat and vulnerability assessment is well known. The General Accounting Office (GAO), national commissions, and prominent scholars have all recommended the use of such analyses well before September 11, 2001.¹² The House Democratic Caucus wrote legislation in 2001 calling for "an assessment of terrorist threats within the United States and the territories," and calling for "a prioritization of the risks against the United States and a forecast of the costs and implications of possible responses to those threats" to be completed by May 2003.¹³

While DHS has begun to identify and catalogue vulnerabilities and is receiving threat assessments from TTIC, it has not completed a threat and vulnerability assessment to understand our most critical weaknesses, inform protective measures throughout the country, and guide the strategic policy of the Department. Such an assessment was included in legislation approved on a bipartisan basis by the House Select Committee on Homeland Security (Select Committee).¹⁴

¹¹ U.S. House, Select Committee on Homeland Security, *Review of Homeland Security's Financial Accountability and Performance Evaluation Process to Examine Waste, Fraud, and Abuse* Hearing, October, 8 2003.

¹² See, for example, (a) GAO, *Combatting Terrorism: Action Taken but Considerable Risks Remain for Forces Overseas*, NSIAD-00-181, (Washington: U.S. General Accounting Office, July 19, 2000); (b) Center for Strategic and International Studies, "Defending America in the 21st Century: New Challenges, New Organizations, and New Policies, Executive Summary of Four Working Group Reports on Homeland Defense," (Washington, D.C.: CSIS, 2000), 9, 13; (c) Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Toward a National Strategy for Combating Terrorism*, Second Annual Report to the President and the Congress, Washington, D.C., December 15, 2000, 8.

¹³ Bioterrorism Protection Act of 2001, H.R. 3255 §401, introduced by Representative Robert Menendez.

¹⁴ See House Report 108-358 accompanying H.R. 2886, the Department of Homeland Security Financial Accountability Act, November 12, 2003. The legislation would "require DHS to develop and annually update a comprehensive national homeland security strategy based on an assessment of risks from terrorism; a prioritization of those risks; the homeland security capabilities necessary to deter, prevent, mitigate, and respond to acts of terrorism and implement the strategy; the adequacy of those capabilities; the long and short term actions necessary to promote homeland security; the priorities guiding resource allocations included in the President's annual budget request for homeland security; and other information necessary for developing a comprehensive national strategy." 11.

SECURITY RECOMMENDATION

The DHS should conduct, complete, and implement a comprehensive threat and vulnerability assessment, and should have such an assessment completed as soon as possible, but not later than October, 2004. This assessment should go beyond critical infrastructure to catalogue all terrorist threats to all potential homeland targets. Once completed, and on a continuing basis, the assessment should influence all homeland security spending across the federal government.

SECURITY GAP: Information Sharing among Federal, State, and Local Governments Must Be Enhanced.

The front lines of homeland security are our local communities, and most of the targets that terrorists might attack are protected by state and local officials. These state and local actors are critical to our national homeland security, capable of both detecting the presence or activities of terrorists and predicting potential terrorist targets. But state and local officials and organizations can only fill these roles adequately if they are given terrorist threat information, and if the federal government treats them as true partners in the collection and dissemination of information about potential terrorists. When the federal government receives and subsequently analyzes terrorism information, this information—or an appropriate, actionable summary of the information—must be provided to the state and local officials who are responsible for protecting their communities.

State and local officials have confirmed that they are looking to DHS for information about the terrorist threat within their jurisdiction or state, in part to help them develop their own risk assessments.¹⁵ The importance of such information is underscored by James Kallstrom, the Senior Advisor to the Governor of New York for Counterterrorism, who stated that “the federal government must provide the police officer on patrol with the ability, under controlled and auditable circumstances, to request a comprehensive search of federal databases, [...] in order to receive a ‘green light – yellow light – red light’ indication regarding a subject of interest’s possible link to terrorist activity.”¹⁶

- **Information Sharing Procedures**

Many state and local government officials have grown increasingly frustrated at the perceived lack of progress at the federal level in sharing information, the dearth of actionable intelligence coming from federal sources, and the lack of transparency and feedback regarding how the information they provide is being utilized.¹⁷ The GAO has found that officials from federal agencies, states, and cities generally do not consider the current process of sharing information to protect the homeland to be effective. Indeed, only 35 percent of the survey respondents reported

¹⁵ Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Fifth Annual Report to the President and Congress*, (Arlington, VA: RAND, December 15, 2003), 32.

¹⁶ U.S. House, Select Committee on Homeland Security, *DHS Information Sharing with Federal, State and Local Government Entities Hearing*, July 24, 2003.

¹⁷ Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Fifth Annual Report to the President and Congress*, (Arlington, VA: RAND, December 15, 2003), 3.

that sharing with the federal government was “effective” or “very effective.”¹⁸ Massachusetts Governor Mitt Romney succinctly summarized the problems with the Administration’s existing and proposed information sharing systems, stating, “Another challenge we face in information sharing is ensuring that there is an appropriate exchange of information between the federal government and the state and local officials who may be able to use that information. ... The bottom line is that a more effective liaison must be established between the FBI, CIA, DHS and other national security agencies if we are to maximize our nation’s investment in intelligence.”¹⁹ According to the Markle Foundation Task Force on National Security in the Information Age (Markle Foundation Task Force), DHS has “not gotten very far in putting in place the necessary staff or framework for analyzing information and sharing it broadly among the relevant federal, state, and local agencies.”²⁰

The Homeland Security Act directs the IAIP Directorate to “disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal Government with responsibilities relating to homeland security, and to agencies of state and local governments and private sector entities with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.”²¹ The Homeland Security Act further required the President to submit a report to Congress on the processes and procedures used by the federal government to share information with state and local officials not later than November 25, 2003.²² The President, through Executive Order, assigned the task of setting information sharing procedures to the Secretary of Homeland Security, suggesting that the DHS should be the lead federal agency for sharing information with state and local governments.²³ Although the Intelligence Authorization Act for Fiscal Year 2004 extended this deadline to February 13, 2004,²⁴ Congress has yet to receive this critical report.

In addition, the FBI shares information with state and local officials, primarily those in the law enforcement community, through its 84 Joint Terrorism Task Forces (JTTFs).²⁵ Although steps have been taken at the federal, state, and local levels to broaden the sharing of terrorist threat data among government agencies at all levels, the sharing of such information between relevant agencies at different levels of government has been only marginally improved since the creation of DHS and remains haphazard.²⁶

Multiple hearings of the Select Committee have revealed that there is no clear delineation between the information disseminated through the FBI and that which should be disseminated by

¹⁸ GAO, *Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened*, GAO-03-760, (Washington: U.S. General Accounting Office, August 27, 2003), 4.

¹⁹ U.S. House, Select Committee on Homeland Security, *First Responders: How States, Localities and the Federal Government Can Strengthen Their Partnership to Make America Safer* Hearing, July 17, 2003.

²⁰ Markle Foundation, *Creating a Trusted Network for Homeland Security: Second Report of the Markle Foundation Task Force*, (New York: Markle Foundation, December 2, 2003), 3.

²¹ “Homeland Security Act of 2002” (P.L. 107-296, § 201(d)(9)), U.S. Statutes at Large. 116 Stat. 2147.

²² “Homeland Security Act of 2002” (P.L. 107-296, § 892-893), U.S. Statutes at Large. 116 Stat. 2253-56

²³ The White House, “Executive Order: HSIS,” July 29, 2003.

<http://www.whitehouse.gov/news/releases/2003/07/20030729-10.html>.

²⁴ “Intelligence Authorization Act for Fiscal Year 2004” (P.L. 108-177, §316(b)), U.S. Statutes at Large.

²⁵ U.S. Department of Justice Office of the Inspector General, Audit Division, “The Federal Bureau of Investigation’s Efforts to Improve the Sharing of Intelligence and Other Information,” Audit Report 04-10, December 2003, 41.

²⁶ Markle Foundation, *Creating a Trusted Network for Homeland Security: Second Report of the Markle Foundation Task Force*, (New York: Markle Foundation, December 2, 2003), 2.

DHS.²⁷ The division of responsibilities at the federal level also appears to be unclear to state and local officials. According to George Foresman, Deputy Assistant to the Governor of Virginia for Commonwealth Preparedness, information is being provided to state and local officials without coordination at the Federal level.²⁸ He has received information from a JTTF, and then found that DHS officials were unaware of the same information.²⁹ If there is a need for these agencies to share information through separate channels, that need has not been articulated. This lack of established procedures for sharing information among the federal, state, and local levels will result in information sharing continuing to be on an *ad hoc* basis. Without established procedures, state and local officials may continue to receive conflicting information and not be in a position to rely on the credibility of information.³⁰

Finally, the federal government lacks a broad information network to draw upon, bring together, and distribute information to all homeland security stakeholders. The Markle Foundation Task Force has proposed such a network to document, share, analyze, and audit intelligence reports on the terrorist threat.³¹ Such a system would include information from classified intelligence sources and non-governmental personnel, including operators of critical infrastructure and experts in terrorist-related fields. The technology for such a system is currently available commercially.

SECURITY RECOMMENDATION

The Administration should name DHS as the lead federal agency for sharing terrorist threat information with state and local governments, while the FBI should share terrorist threat information for criminal investigation purposes through its JTTFs. The DHS should complete the report mandated by Congress regarding the development of information sharing procedures, and should develop a capacity to share terrorism-related information quickly with state, local, and private sector entities in order to optimize their capability to detect and respond to would-be terrorists. Congress should provide constant oversight on this issue and pressure Executive Branch agencies to take the necessary steps to share information with their state and local counterparts.

The DHS should establish clear mechanisms for responding to requests for threat and vulnerability information from state and local officials, develop a consistent process for receiving
(Continued on the following page)

²⁷ (a) U.S. House, Select Committee on Homeland Security, *DHS Information Sharing with Federal, State and Local Government Entities* Hearing, 24 July 2003; (b) U.S. House, Select Committee on Homeland Security, *First Responders: How States, Localities and the Federal Government Can Strengthen Their Partnership to Make America Safer* Hearing, July 17, 2003.

²⁸ U.S. House, Select Committee on Homeland Security, *DHS Information Sharing with Federal, State and Local Government Entities* Hearing, July 24, 2003.

²⁹ Ibid.

³⁰ At the July 24 hearing, Mr. Foresman testified that in one instance, he received information from DHS which was immediately attacked by another federal agency as "old news." Mr. Foresman was then faced with trying to validate the information through unofficial channels. U.S. House, Select Committee on Homeland Security, *DHS Information Sharing with Federal, State and Local Government Entities* Hearing, July 24, 2003.

³¹ Markle Foundation, *Creating a Trusted Network for Homeland Security: Second Report of the Markle Foundation Task Force. Part Two: Working Group Analyses, Working Group I: Networking of Federal Government Agencies with State and Local Government and Private Sector Entities*, (New York: Markle Foundation, December 2, 2003).

information from state and local officials, and establish a culture that makes responding to such requests a priority.³²

The Administration should charge DHS with leading the implementation of the federal government's efforts to create an information network as proposed by the Markle Foundation Task Force.

- **Security Clearances**

The lack of security clearances at the state and local levels continues to inhibit the widespread dissemination of more general strategic intelligence beyond a very limited number of individuals.³³ This problem was highlighted by Governor Romney in a hearing before the Select Committee when he stated, "One way to address the intelligence-sharing dilemma is for security clearances to be standardized and reciprocal between agencies and levels of government—perhaps within the Department of Homeland Security. There is also a need to process federal security clearances more expeditiously. Some states have waited over a year for vital security clearances for their law enforcement agents."³⁴ In the fall of 2003, DHS announced that, in addition to state governors, five senior state officials would be issued security clearances to receive intelligence regarding specific threats or targets. (These clearances are in addition to the security clearances to be issued to public health officials.) However, there is concern among state officials that the number of security clearances allocated may still be too few to account for all their needs.³⁵ This DHS policy also does not meet the need for personnel with security clearances in local jurisdictions, especially large metropolitan areas.

SECURITY RECOMMENDATION

The Administration should develop a new regime of clearances and classification of intelligence and other information for dissemination to states, localities, and the private sector. This new regime should provide the widest possible distribution to local and state responders in a form that conveys meaningful and useful information. Such a process could also prove to be less expensive and less time consuming for background investigations and the granting of clearances, as well as more effective in disseminating valuable intelligence that might help prevent a terrorist attack.³⁶

³² Ibid.

³³ Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. *Fifth Annual Report to the President and Congress*, (Arlington, VA: RAND, December 15, 2003), 5.

³⁴ U.S. House, Select Committee on Homeland Security, *First Responders: How States, Localities and the Federal Government Can Strengthen Their Partnership to Make America Safer* Hearing, July 17, 2003.

³⁵ Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Fifth Annual Report to the President and Congress*, (Arlington, VA: RAND, December 15, 2003), 32.

³⁶ Ibid, 33.

SECURITY GAP: There is Still No Comprehensive, Integrated Terrorist Watch List.

Access to a comprehensive watch list is important to nearly every piece of the homeland security effort. Officials at our embassies reviewing visa applications, customs and immigration inspectors at air, land, and sea ports of entry, and law enforcement officials patrolling our streets need prompt access to terrorist watch list information in order to identify potential terrorists and react accordingly.

However, the lack of an integrated terrorist watch list has long been a critical shortfall in homeland security and the war against al Qaeda and other terrorist groups. Even before September 11, 2001, information on terrorist suspects was disorganized and poorly used. Two of the September 11 hijackers, Khalid al-Mihdhar and Nawaf al-Hazmi, should have been placed on watch lists on at least three occasions.³⁷ The effective use and dissemination of accurate watch list information would likely have allowed authorities to prevent these two from boarding American Airlines flight 77, which was flown into the Pentagon.

The Congressional Joint Inquiry recommended that, "Congress and the Administration should ensure the full development of a national watch list center that will be responsible for coordinating and integrating all terrorist-related watch list systems."³⁸ In April, 2003, the GAO reported that the U.S. Government was still using 12 separate watch lists maintained by nine different federal agencies and recommended that these watch lists be integrated to provide a stronger homeland security tool.³⁹

Following the September 11 attacks, President Bush gave the White House Office of Homeland Security responsibility for overcoming interagency turf battles by coordinating all executive branch efforts to prepare for terrorist attacks, including the preparation of an integrated watch list.⁴⁰ Yet nothing had been accomplished by July, 2002, when the Administration's *National Strategy for Homeland Security* pledged to "build and continually update a fully integrated, fully accessible terrorist watch list" and placed responsibility for watch list integration with the FBI.⁴¹ The FBI soon transferred responsibility back to the White House, after which, the White House assigned the task to the new DHS.⁴² Finally, on September 16, 2003, the Administration announced its intention to create a Terrorist Screening Center (TSC) to address the watch list problem. According to the White House press releases, the TSC will "consolidate terrorist watch lists and provide 24/7 operational support for thousands of federal screeners across the country and around the world."⁴³

³⁷ House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, *Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001*, House Report 107-792 and Senate Report 107-351, December, 2002.

³⁸ Ibid.

³⁹ GAO, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, GAO-03-322, (Washington: U.S. General Accounting Office, April 15, 2003).

⁴⁰ The White House, "Executive Order 13228," October 8, 2001.

<http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html>.

⁴¹ Office of Homeland Security, *National Homeland Security Strategy*, July, 2002, 26.

⁴² GAO, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, GAO-03-322, (Washington: U.S. General Accounting Office, April 15, 2003).

⁴³ The White House, "New Terrorist Screening Center Established," September 16, 2003.

<http://www.whitehouse.gov/news/releases/2003/09/20030916-8.html>.

The Democratic Members of the Select Committee issued a report on November 21, 2003, outlining ten characteristics necessary for a fully operational and appropriate unified watch list.⁴⁴ However, despite the nearly 26 months between September 11, 2001, and December 1, 2003, the TSC was not fully operational when it officially began its work on December 1.⁴⁵ Existing shortcomings include:

- Less than 20 percent of the records – from only a few of the existing watch lists – have been integrated into the TSC system, so that routine criminal background checks by federal, state, and local law enforcement will miss many of the individuals the government suspects of terrorist involvement.
- As of mid-January, 2004, only 30 people (including contractors and detailees) were staffing the TSC, despite TSC representatives' indications that they need more personnel to carry out their mission.
- Despite the Administration's announcement in September 2003 that the TSC would "consolidate terrorist watchlists," the TSC is still not in a position to create a comprehensive integrated database. Basic information sharing and data use issues remain unresolved between the TSC and the other federal agencies that own the 12 separate watch lists.
- Other federal agencies are not yet working with the TSC as intended. The TSC was not used to run checks against passenger lists on Air France and other airlines that led to cancelled and delayed flights in December, 2003.

The TSC currently plans to have a single, consolidated database completed by the end of summer 2004, at least six months after the TSC began operations.⁴⁶ While a positive step, TSC officials acknowledge that there are lists of known and suspected terrorists scattered throughout federal agencies beyond the original 12 identified by GAO that will not be integrated by that time.⁴⁷ Furthermore, there are several other steps that the TSC must take in order to have a full operational capability. These include building a full staff complement to regularly maintain the integrated watch list and provide support to TSC customers, completing agreements with other agencies for manipulating information, developing a standard and accessible process for watch list appeals, and incorporating advanced software to allow the watch list database to recognize name variants and aliases and conduct additional pattern recognition.

⁴⁴ Democratic Members of the House Select Committee on Homeland Security, "Keeping Terrorists Out of America by Unifying Terrorist Watch Lists," November 2003.

http://www.house.gov/hsc/democrats/pdf/press/031124_TSC_Report_and_Cover_final.pdf.

⁴⁵ According to FBI Assistant Director Eleni Kalisch on December 18, 2003, "The TSC is currently in a test phase of the consolidated database application which will assimilate available terrorist information into one database." Letter to Congressman Jim Turner, Ranking Member, House Select Committee on Homeland Security from Eleni Kalisch, Assistant Director of the Federal Bureau of Investigation, Office of Congressional Affairs, December 18, 2003, 2.

⁴⁶ Secretary Tom Ridge testified before the Senate Committee on Government Affairs on February 9, 2004 that names will be "aggregated into a single database" by the end of summer 2004. See also testimony of Donna A. Bucella, Director, Terrorist Screening Center, to the National Commission on Terrorist Attacks Upon the United States. January 26, 2004.

⁴⁷ Briefing from TSC officials to Select Committee staff, January 15, 2004.

SECURITY RECOMMENDATION

The Administration should exert the leadership required to ensure the full cooperation from all agencies to create and properly use the Terrorist Screening Center's unified terrorist watch list. As described in the report by the Democratic Members of the Select Committee on November 21, 2003, the watch list should be a comprehensive listing of all the persons suspected of involvement in terrorist activity, and the TSC should have unfettered access to all information needed to compile and maintain such a list. All other capabilities needed to compile and operate a unified watchlist effort should be achieved as soon as possible.

Preventing Attacks by Securing Nuclear Materials

Despite the United States' participation in various threat reduction programs for more than a decade, there are still hundreds of tons of unsecured nuclear, chemical and biological weapons and materials worldwide. Securing them is critical to prevent them from falling into the hands of terrorists. Yet even after learning of terrorist interest in acquiring weapons of mass destruction, the Administration has not pursued an aggressive strategy to secure these hazardous stockpiles within the former Soviet Union, as well as stockpiles located in other countries. Our unilateral efforts need to be accelerated, including efforts to control radiological materials within our borders, and the United States should lead a global coalition devoted to reducing this dramatic security threat.

Though securing weapons of mass destruction (WMD) has been a goal since the dawn of the nuclear age, and became increasingly so with the break-up of the former Soviet Union, this potential threat crystallized with the September 11, 2001, terrorist attacks on the United States. These attacks showed that al Qaeda's capacity for killing is limited only by the power of the weapons they are able to obtain. Evidence discovered in Kabul, Afghanistan – including crude bomb design drawings and extensive downloaded materials on nuclear weapons – confirmed al Qaeda's interest in obtaining a nuclear weapon.⁴⁸ Indeed, Osama Bin Laden has said that gaining nuclear weapons is “a religious duty.”⁴⁹ President Bush stated that “terrorists armed with weapons of mass destruction pose the ‘most horrifying’ danger civilization faces, and he has said that keeping WMD out of terrorists’ hands is his Administration’s ‘highest priority’.”⁵⁰

Former Senator Sam Nunn has clearly articulated the simple reality of the WMD problem when he said that:

“The most effective, least expensive way to prevent nuclear terrorism is to secure nuclear weapons and materials at the source. Acquiring weapons and materials is the hardest step for the terrorists and the easiest step for us to stop. By contrast, every subsequent step in the process is easier for the terrorists to take, and harder for us to stop.”⁵¹

Current figures show there are 105 nuclear sites in Russia with 243 buildings that need assistance improving their security.⁵² According to the Department of Energy's National Nuclear Security

⁴⁸ Robert J. Einhorn and Michele Flournoy, *Protecting Against the Spread of Nuclear, Biological, and Chemical Weapons, An Action Agenda for The Global Partnership*, Center for Strategic and International Studies, January 2003, 9.

⁴⁹ “Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001,” *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, December 2002, 71.

⁵⁰ Matthew Bunn, Anthony Wier and John Holdren, *Controlling Nuclear Warheads and Materials, A Report Card and Action Plan*, Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, March 2003, vii.

⁵¹ *Ibid.*, ix.

⁵² Amy F. Woolf, *Nonproliferation and Threat Reduction Assistance: US Programs in the Former Soviet Union*, Congressional Research Service, October 23, 2003, 24.

Administration, "these sites contain approximately 600 metric tons of nuclear materials, enough for around 41,000 nuclear warheads."⁵³

SECURITY GAP: Nuclear Weapons and Materials In The Former Soviet Union Are Still Not Secure.

Not only do we know that terrorists are seeking materials to construct weapons of mass destruction, we also know where they are looking – the former Soviet Union. While a number of countries possess significant stocks of nuclear materials, the largest concentration is in the former Soviet Union, with 99 percent located in Russia and smaller amounts in Kazakhstan, Belarus, Ukraine and Uzbekistan.

Since the fall of the former Soviet Union, Russia retains more than 20,000 strategic nuclear warheads at 123 nuclear weapons storage sites, and a massive 1,350 metric tons of highly enriched uranium and weapons-grade plutonium remain dispersed in a variety of forms in numerous locations within what remains the largest network of nuclear facilities in the world, employing more than one million poorly paid workers.⁵⁴ Many experts estimated that it only takes a few kilograms of plutonium, or several times that amount of highly enriched uranium (HEU), to make a nuclear weapon.

Russia also possesses thousands of tactical nuclear weapons that, in some respects, are more dangerous than their strategic partners. Their small size and the absence of electronic locks that could be used to secure them contribute to their vulnerability to theft or unauthorized use. Some of these weapons are small enough to fit into a backpack but powerful enough to destroy a small city. They have never been subject to any arms control agreement or monitoring, so we do not know how many there are in the Russian inventory, where they are located or how they are protected. All of this makes them extremely dangerous if they fall into the hands of terrorists.⁵⁵

Despite improvements in the Russian economy, the state-run defense, biotechnology, and nuclear industries remain strapped for funds even as Moscow looks to them for badly needed foreign exchange through exports. Accordingly, many experts and the intelligence community have continued to express grave concerns about the diversion or theft of know-how, materials or weapons from Russia and other parts of the former Soviet Union.⁵⁶ They have found that many of the counter-measures used by the Russians are antiquated, inadequate for dealing with the "insider threat" and insufficiently staffed and funded.⁵⁷

Thefts of weapons-useable material in quantities sufficient to make a crude nuclear device have already occurred. How many thefts, the total amount stolen and, most importantly, by whom, are still in some doubt. The International Atomic Energy Agency contends that over the last decade there have been 18 confirmed thefts involving plutonium or enriched uranium.⁵⁸ The Center for Nonproliferation Studies of the Monterey Institute of International Studies has maintained an open source database of reported nuclear trafficking incidents in the former Soviet Union. They record 14 confirmed "proliferation-significant cases" involving the theft or attempted theft of

⁵³ Ibid.

⁵⁴ Einhorn and Flournoy, vii.

⁵⁵ Dr. Nikolai Sokov, *Tactical Nuclear Weapons Issue Brief*, Center for Nuclear Studies, May 2002.

⁵⁶ National Intelligence Community, *Annual Report to Congress on the Safety and Security of Russian Nuclear Facilities and Military Forces*, February 2002, 3.

⁵⁷ Ibid.

⁵⁸ Einhorn and Flournoy, 9-10.

HEU or plutonium. In five of these cases, the material made it out of the former Soviet Union. In one case involving the theft of two kilograms of HEU from a research institute in Sokhumi, Georgia, the whereabouts of the stolen material remains unknown.⁵⁹

The Central Intelligence Agency, in its 2002 report on the security of Russian nuclear facilities, agreed with those assessments. It determined that “weapons-grade” and “weapons-usable” materials have been stolen from Russia. Moreover, it found that:

“Undetected smuggling has occurred, although we do not know the extent or magnitude of such thefts. Nevertheless, we are concerned about the total amount of material that could have been diverted over the last 10 years.”⁶⁰

In the early 1990’s, former Senator Sam Nunn saw the need to take action to identify and secure loose nuclear material. He worked with Senator Richard Lugar to create the Cooperative Threat Reduction Programs – commonly called CTR or “Nunn-Lugar.” CTR, which is funded through the Department of Defense, has evolved from an initial emergency response after the breakup of the former Soviet Union, “to a more comprehensive threat reduction and nonproliferation effort, to a broader program seeking to keep nuclear, chemical, and biological weapons from leaking out of the former Soviet Union and into the hands of rogue nations and terrorist groups.”⁶¹

The Department of Energy has developed a number of programs to work in conjunction with CTR in the former Soviet Union. In 1995, the Department of Energy launched the Material Protection, Control and Accounting Program to help secure former Soviet weapons-usable nuclear materials. It later created the Initiative for Proliferation Prevention Program and the Nuclear Cities Initiative to engage unemployed weapons scientists in various peaceful commercial projects. The Department also has two other initiatives to reduce Soviet stockpiles of weapons useable material by converting this material into fuels that cannot be used as weapons.

Since the early 1990s, the United States has been actively engaged in attempts to help the Russians secure their nuclear weapons arsenal. These efforts include: decreasing vulnerability to theft of nuclear stockpiles; enhancing the safety of nuclear facilities and weapons-grade material; and curbing the diffusion of nuclear-related technologies and equipment. Despite these initiatives, a 2001 bipartisan panel report to the Secretary of Energy concluded that uncontrolled nuclear weapons material in the former Soviet Union is “the most urgent unmet national security threat to the United States today.”⁶² This Russia Task Force, chaired by former Senate Majority Leader Howard Baker and former White House Counsel Lloyd Cutler, was explicit in its concern about the potential for these weapons and materials being stolen and sold to terrorists or hostile nation states and used against American troops abroad or citizens at home.⁶³ It recommended that the U.S. spend up to \$30 billion over the next eight to ten years to improve the security of Russian nuclear stockpile.

⁵⁹ Scott Parrish, *Illicit Nuclear Trafficking in the NIS Issue Brief*, Center for Non-Proliferation Studies, March 2002.

⁶⁰ National Intelligence Community, 3.

⁶¹ “Nonproliferation and Threat Reduction Assistance: U.S. Programs in the Former Soviet Union.”

⁶² John T. Cappello, Gwendolyn M. Hall and Stephen P. Lambert, *Tactical Nuclear Weapons: Debunking the Mythology*, INSS Occasional Paper 46 (USAF Academy, CO: USAF Institute for National Security Studies), 12.

⁶³ Amy F. Woolf, “Nunn-Lugar Cooperative Threat Reduction Programs: Issues for Congress,” Congressional Research Service, Updated March 6, 2002, 4-5.

The urgency of the task remains. To date, even initial “rapid upgrades” such as installing detectors on doors, putting material in steel cages, and counting the amount of material present have been accomplished for only 40 percent of the potential bomb material in Russia. Less than one-seventh of Russia’s stockpile of highly enriched uranium has been destroyed.⁶⁴ And only 23 percent of Russia’s potentially vulnerable material has received “comprehensive upgrades,” that is, a complete modern security and accounting system.⁶⁵ The Administration, however, has not accelerated efforts to secure loose nuclear material in Russia. Funding for “Nunn-Lugar” CTR programs has remained relatively flat over the last several years at approximately \$1 billion a year.

In its fiscal year 2005 budget request, the Administration seeks \$409.2 million for the DOD portion of the CTR programs. This request represents a \$41.6 million reduction for the CTR program overall, from the \$450.8 million appropriated by Congress for fiscal year 2004. Much of the decrease comes in the area of chemical weapons destruction and dismantlement, from \$200.3 million to \$158.4 million. Monies for other important components of the CTR program, such as warhead storage security and enhanced security for Russian and former Soviet Union biological sites, remain largely stable or with slight increases.⁶⁶ Likewise, the Department of Energy’s fiscal year 2005 budget request of \$470 million for nonproliferation activities in Russia and the former Soviet Union is largely a status-quo proposal, providing no new funding initiatives and recommending a few minor budget cuts from last year’s appropriation of \$475 million.⁶⁷

SECURITY RECOMMENDATION

Because of the seriousness of this problem, the pace of efforts to secure loose nuclear material should be accelerated. We should move faster and take stronger measures to secure loose nuclear material before it falls in the wrong hands. The United States should meet the goals of the Baker-Cutler Commission and triple the resources spent to improve nuclear security by spending \$30 billion over the next ten years to improve nuclear stockpile security.

SECURITY GAP: Nuclear Weapons and Materials Outside the Former Soviet States are Not Secure.

Though the largest stock of unsecured nuclear material is in Russia and some of its former Republics, the threat posed by loose nuclear material extends far beyond these former Soviet states. These nations possess materials, weapons, or knowledge that can leak out beyond their borders.⁶⁸ Some 20 tons of HEU exist at 130 civilian research facilities in 40 countries, many of

⁶⁴ “New Report Recommends Seven Urgent Steps to Reduce Terrorist Threat from Nuclear Weapons and Materials,” *Nuclear Threat Initiative, Press Release*, May 20, 2002.

⁶⁵ Matthew Bunn, “Preventing Nuclear Terrorism: A Progress Update,” Belfer Center for Science and International Affairs, October 22, 2003. See also, Bunn, Wier, and Holdren, 65.

⁶⁶ William Hoehn, “Preliminary Analysis of the U.S. Department of Defense’s Fiscal Year 2005 Cooperative Threat Reduction Budget Request,” Russian American Nuclear Security Advisory Council, February 10, 2004.

⁶⁷ William Hoehn, “Preliminary Analysis of the U.S. Department of Energy’s Fiscal Year 2005 Nonproliferation Budget Request,” Russian American Nuclear Security Advisory Council, February 4, 2004.

⁶⁸ Amy Woolf, 40.

which have no more security than a night watchman and a chain link fence.⁶⁹ One such facility is located in the highly unstable nation of the Congo.

The majority of these materials are the result of Cold War era programs in which the U.S. and Soviet Union curried favor in the developing world by assisting in the building of nuclear research reactors. A recent review by the Department of Energy Inspector General highlights serious problems related to the security and safekeeping of this material which could be used to build a nuclear weapon or “dirty bomb.”⁷⁰

The Inspector General found that the Department of Energy’s program to recover this material is limited to foreign research reactors which only cover 5,200 kilograms of the approximately 17,500 kilograms of U.S.-produced material overseas.⁷¹ Moreover, the Inspector General concluded that this program would only recover one half of those 5,200 kilograms due to management and funding shortcomings.⁷² Significantly, the Inspector General discovered that the Energy Department has no plan to address and recover the remaining 12,300 kilograms of HEU used in fast reactors and other special reactors.⁷³

The Inspector General also noted that at least 56 kilograms of U.S.-produced HEU was exported to four countries now considered “sensitive” security risks which were not participating in Energy’s attempts to repatriate the material. Accordingly, the Inspector General noted that the continued failure of the Energy Department to recover more of this HEU created a growing risk of diversion to groups and governments hostile to the United States for use in nuclear weapons.⁷⁴

The international community has also recently acknowledged that unsecured nuclear weapons and materials are a global problem. In June 2002, the U.S. joined the leaders of the G-8 nations to create the “G-8 Global Partnership Against the Spread of Weapons and Materials of Mass Destruction” (Global Partnership). The G-8 has since expanded to include non-G8 countries. The “10+10 over 10” initiative committed the G-8 to a spending program whereby the U.S. would contribute \$10 billion over ten years (through programs such as “Nunn-Lugar” in the Departments of Energy, Defense, and State) and the other G-7 nations together would provide up to \$10 billion over 10 years. The U.S. spending pledge, however, is not an increase compared to what it was planning to spend before the September 11 terrorists attacks.⁷⁵

At the Evian summit held on the one year anniversary of the Global Partnership, the G-8 leaders announced they had received pledges totaling \$18 billion towards their goal of \$20 billion over 10 years. They also pledged to expand the list of recipients beyond the former Soviet Union states. Pakistan, for example, was cited as a state needing assistance “because of its location, the

⁶⁹ Bunn, Wier and Holdren, 3.

⁷⁰ U.S. Department of Energy Inspector General, *Recovery of Highly Enriched Uranium Provided to Foreign Countries*, Audit Report DOE/IG-0638, February 2004.

⁷¹ This program, now known as the Foreign Research Reactor Sent Nuclear Fuel Acceptance Program (Acceptance Program), is voluntary and funded, to a large extent, by countries that participate in it. It is currently planned to end in May, 2006, Ibid., 1.

⁷² Ibid, 2-4.

⁷³ Ibid.

⁷⁴ Ibid, 4.

⁷⁵ “An American Security Policy: Challenge, Opportunity, Commitment,” National Security Advisory Group, William J. Perry, Chair, July 2003, 13-14.

nature of its relationship to the Taliban and al Qaeda, and its weapons of mass destruction programs.”⁷⁶

However, given the nuclear materials outside of the former Soviet Union that remain insecure, more needs to be done. A small step toward recognizing the global nature of insecure nuclear materials threat was taken when last year Congress permitted \$50 million of unobligated CTR funds to be used for proliferation emergencies outside the former Soviet Union.⁷⁷

SECURITY RECOMMENDATION

The Administration should accelerate its efforts to recover or secure the thousands of kilograms of HEU that the United States shipped to other countries during the Cold War.

The U.S. commitment of \$10 billion over ten years to address the threat from unprotected materials and weapons of mass destruction is an important step forward but is only a “status quo” proposal – no significant increase from what our country had already planned to spend pre-September 11. The U.S. contribution of \$10 billion over the next decade should be the floor, not the ceiling, of our commitment to address this problem. We should encourage the G-8 to also expand their level of contributions since the threat from terrorists possessing WMDs is an international threat, not limited to any one country. Moreover, we should encourage greater participation by other countries in support of the Global Partnership as well as expansion of the list of recipients to include those nations that pose a substantial risk of diversion of WMD materials, technology or know-how. Congress should authorize CTR funds to be used for threats outside the former Soviet Union.

SECURITY GAP: Sources of Radiological Materials That Can be Used for “Dirty Bomb” Attacks Are Not Secure.

The catastrophic attacks of September 11, 2001, highlighted the nation’s vulnerability to unconventional forms of terrorism. One such threat is the use of commercially available radiological material in the construction of a “dirty bomb.” Though not weapons of mass destruction, such bombs, or radiological dispersion devices (RDDs – the technical term for “dirty bombs”), are weapons of mass disruption that can cause debilitating economic and environmental damage, as well as wide-spread panic and fear.⁷⁸

Recent press revelations have disclosed that the FBI has warned law enforcement over the past year that terrorists were interested in obtaining radiological materials to create a dirty bomb,⁷⁹

⁷⁶ Sharon Squassoni, “Nuclear Threat Reduction Measures for India and Pakistan,” Congressional Research Service, Updated May 5, 2003, 1.

⁷⁷ Senator Richard Lugar’s keynote address to a symposium sponsored by the Embassy of Kazakhstan and the Nuclear Threat Initiative, December 16, 2003.

⁷⁸ Radioactive material that could be used to construct a dirty bomb include: cobalt-60, strontium-90, cesium-137, iridium-192, and americium-241. Among other things, these materials are used to treat cancer, sterilize food and medical instruments, and detect flaws in pipelines and other types of metals.

⁷⁹ John Solomon, “Congress, Energy Department Document Lost Radioactive Material, Terror Concern,” Associated Press, November 10, 2003. See also, Joby Warrick, “Study Raises Projection for ‘Dirty Bomb’ Toll,” *Washington Post*, January 13, 2004, A2.

and its potential use was one of the reasons for the nation's fifth "code orange" alert issued on December 21.⁸⁰ The U.S. Coordinator for Counter Terrorism, Ambassador-at-Large Cofer Black said, while attending the February 2004 anti-terror summit in Indonesia, that U.S. officials are "killing themselves" to make sure terrorists don't get a so-called "dirty bomb."⁸¹

A dirty bomb can be produced by using explosives in combination with radioactive material. Much of the radioactive material used in these devices is encapsulated or sealed in metal to prevent dispersal. A dirty bomb would use explosives in combination with these "sealed sources" to disperse the material upon detonation. The explosion itself will cause the greatest amount of immediate injuries, fatalities, and property damage. Those in close proximity to the explosion can be exposed to radiation for an extended period of time and potentially be at risk of cancer over the long-term.⁸²

Dirty bombs also have the potential to contaminate many city blocks from the site of an explosion causing substantial economic loss and clean-up costs. A recent report done for the National Defense University estimates that the economic impact from a successful RDD attack in a major metropolitan area would likely equal or even exceed the \$41 billion cost of the September 2001 al Qaeda attacks in New York City and Washington, D.C.⁸³

Since 1999, federal investigators have documented 1,300 cases in which radiological material (sealed sources) has been lost, stolen or abandoned inside the U.S.⁸⁴ The Nuclear Regulatory Commission estimates that approximately one licensed U.S. source is lost every day of the year, and these sources have "escaped proper control and their locations are unknown."⁸⁵ The General Accounting Office and others studying this problem have issued these findings:

- The most likely route for terrorist acquisition of intermediate quantities of radioactive materials is through open and legal purchase from a legitimate supplier.⁸⁶
- The actual number of radioactive sources is unknown because no entity keeps track of this information. The Nuclear Regulatory Commission (NRC) estimates there are approximately two million sealed sources in the United States and have been forced to contract with a private investigation firm to help locate the owners of sealed radioactive sources.⁸⁷
- The Department of Energy doesn't have enough secure storage to take control of sources no longer wanted by the current holder.

⁸⁰ John Mintz and Susan Schmidt, "Dirty Bomb Was Major New Year's Worry," *Washington Post*, January 7, 2004, A1.

⁸¹ Steven Gutkin, "US Terror Expert Warns of Dirty Bomb," Associated Press, February 8, 2004.

⁸² A recent National Defense University report notes that some forms of radiological attack "could kill tens or hundreds of people and sicken hundreds or thousands." Peter D. Zimmerman with Cheryl Loeb, "Dirty Bombs: The Threat Revisited," *Defense Horizons*, January 2004, 1.

⁸³ Ibid, 9.

⁸⁴ General Accounting Office, "Federal and State Action Needed To Improve Security of Sealed Radioactive Sources." GAO-03-804, April 2003, 4.

⁸⁵ Zimmerman and Loeb, 2.

⁸⁶ Ibid., 3.

⁸⁷ GAO-03-804, 4.

- The current NRC licensing process leaves sealed sources vulnerable since it approves an applicant to buy sealed sources without any inspection or verification of how the material will be used. Because the process assumes the applicant is acting in good faith, it could take up to a year before the NRC finally conducts an inspection of the applicant.⁸⁸
- There also is no requirement that a foreign supplier selling radioactive material to a U.S. end-user verify the validity of any license submitted by the American purchaser. Likewise, U.S. exporters of radioactive material are not required to notify the competent authorities in the destination country that such material has been shipped or to verify its recipient's bona fides.⁸⁹
- The International Atomic Energy Agency says there are 110 countries without the regulatory infrastructure to adequately protect or control sealed sources.⁹⁰
- A survey of U.S. and international holders of sealed materials reveals the controls vary greatly and are mainly focused on protecting public health and safety rather than on security from theft or misuse.⁹¹

Although the fiscal year 2005 budget provides support for several ongoing programs to assist in nuclear and radiological cleanup, the request for the Radiological Dispersal Devices (RDD) program to secure, consolidate, and dispose of potential radiological weapon sources internationally has been reduced over 20 percent or \$9 million, relative to the \$36 million provided for the current fiscal year.

SECURITY RECOMMENDATION

In order to address the serious threat from a "dirty bomb," the Administration, should, at a minimum, restore funding levels for the RDD program to at least the fiscal year 2004 amounts. The next step to improve our security from such an attack is to conduct a threat assessment that would identify those sources most likely to be used by terrorists. Such an approach would allow both domestic and international authorities to appropriately prioritize their regulatory and security resources. In addition, U.S. and international licensing rules must be refocused from health and safety concerns to address the more pressing security and counter-terrorism realities of today. Specifically, the NRC's licensing rules must be toughened to ensure the bona fides of any purchaser of radiological materials before they can acquire them. The United States should require foreign suppliers to verify that shipments of radioactive materials into the United States are sent to valid license holders. Likewise, U.S. export regulations should ensure that consignees have valid national licenses to receive radiological materials. Finally, radiological screening at our borders should receive the necessary support from the Administration to ensure that such material will be stopped before it can be used as a weapon against the United States.

⁸⁸ Ibid., 22-23.

⁸⁹ Zimmerman and Loeb, 3.

⁹⁰ General Accounting Office, "US and International Assistance Efforts to Control Sealed Radioactive Sources Need Strengthening," GAO-03-638, May 2003, 17. <http://www.gao.gov/atest/d03638.txt>

⁹¹ Ibid., 20.

Preventing Attacks Through Biodefense & Preparedness

Bioterrorism is among the most serious threats to homeland security because of its potential to harm millions and spread massive terror. The Administration has not responded to this threat as aggressively or as comprehensively as is needed, leaving foreign and domestic stores of deadly pathogens unsecured, insufficiently addressing a severely neglected and overtaxed health infrastructure, and providing an incomplete plan to develop new vaccines and treatments to neutralize this threat. A comprehensive approach to bioterrorism requires concerted effort in three areas: prevention, including developing new and strengthening existing programs to secure pathogen stocks around the world; preparedness, including completing a comprehensive biodefense plan, strengthening and better targeting federal public health funding; and protection, developing the ability defend our population through deploying the drugs, vaccines, and diagnostics required to combat infection and illness.

Well before 2001, public health experts warned that biological weapons could serve as the ideal weapon of terror, easily spreading fear and confusion, capable of causing mass casualties, and difficult to trace.⁹² The anthrax attacks of October-November 2001 provided a startling demonstration of the ability of bioterrorism to murder, spread fear, and paralyze infrastructure. U.S. officials believe that al Qaeda is pursuing sophisticated biological weapons.⁹³ A United Nations panel recently declared it is “just a matter of time” before al Qaeda attempts a biological or chemical attack.⁹⁴ Yet, despite a flurry of initiatives over the past two years, serious gaps remain in the endeavor to prevent, deter, and respond to bioterrorism. The Administration has not moved as quickly or aggressively as is required to address this evolving threat, leaving the nation without an effective response.

⁹² (a) D.A. Henderson, “Bioterrorism as a Public Health Threat,” *Emerging Infectious Disease*, 4, no.3 (July-September 1998): 488-492; (b) John Schwartz and Michael Osterholm, *Living Terrors: What America Needs to Know to Survive the Coming Bioterrorist Catastrophe*, (New York: Dell Publishing, 2000); (c) Institute of Medicine, *Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response*, (Washington, D.C.: National Academy Press, 1999).

⁹³ (a) Central Intelligence Agency, *Terrorist CBRN: Materials and Effects*, http://www.cia.gov/cia/reports/terrorist_cbrn/terrorist_CBRN.htm, visited January 22, 2004; (b) Department of Homeland Security, “Maintaining Awareness Regarding Al-Qaeda’s Potential Threats to Homeland,” press release, September 4, 2003, <http://www.dhs.gov/dhspublic/display?content=1442>; (c) Matt Kelley, “Pentagon: Al Qaeda Pursuing Bioweapons,” *Associated Press*, May 23, 2003.

⁹⁴ Vivienne Foley, “U. N. Details Al Qaeda Threat,” CNN.com, November 20, 2003, <http://www.cnn.com/2003/US/11/20/un.alqaeda/>.

Preventing the Use of Biological Weapons

The best means for preventing bioterrorism is to keep dangerous biological materials out of the hands of terrorists. A top government priority should be to minimize the chance dangerous pathogens, such as anthrax, smallpox, or Ebola virus, being deployed against vulnerable populations. Stores of these pathogens, and the expertise to use them as weapons, remain in many sites in the former Soviet Union, in research laboratories throughout the world,⁹⁵ and, increasingly, in research facilities in the United States.⁹⁶

SECURITY GAP: Biological Weapon Sites in the Former Soviet Union Remain Unsecured.

As discussed in a previous chapter, the legacy of Soviet weapons of mass destruction programs, including the largest and most intensive biological weapons program in history, have left dangerous materials and expertise susceptible to theft or appropriation by terrorist groups. Cooperative Threat Reduction programs with Russia and other former Soviet states, managed through several U.S. agencies, were established beginning in 1991 to deal with these threats. However, chronic underfunding and a lack of strong leadership and management have hindered the success of these efforts. Funding for Department of Defense (DOD) security improvements have remained flat at \$55 million since fiscal year 2003.⁹⁷ Meanwhile, the General Accounting Office (GAO) has reported disarray in DOD efforts to secure former biological weapons sites.⁹⁸ After four years, DOD has made limited progress, with security projects underway at only four of 49 known biological sites and with only two sites secured against external threats.⁹⁹ Deficiencies include:

- Lack of assessments of the number, location, pathogen inventory, and current security status of bioweapon sites;
- A lack of a plan or timeframe for completing security upgrades;
- Failure to address “insider” threats that may lead to theft of agents.¹⁰⁰

The Russian government has also been uncooperative in the effort to secure some former bioweapon sites. The Ministries of Defense and Agriculture have blocked access to certain facilities, while the Russian government has rejected the establishment of interagency agreements concerning implementation of security measures.¹⁰¹

GAO has also found that the International Science Centers program, an effort managed by the Department of State and intended to occupy former Soviet weapons scientists in peaceful

⁹⁵ Michael Barletta, Amy Sands, and Jonathan Tucker, “Keeping Track of Anthrax,” *Bulletin of the Atomic Scientists* 58, no. 3 (May/June 2002): 57.

⁹⁶ Brad Knickerbocker, “Concern Over Spread of Biodefense Labs,” *Christian Science Monitor*, September 25, 2003, 2.

⁹⁷ Nuclear Threat Initiative, *Controlling Nuclear Warheads and Materials: Threat Reduction Budgets*, http://www.nti.org/e_research/cnwm/charts/cnm_funding_interactive.asp, visited February 13, 2004.

⁹⁸ U.S. General Accounting Office, *Weapons of Mass Destruction: Additional Russian Cooperation Needed to Facilitate U.S. Efforts to Improve Security at Russian Sites*, GAO-03-482, (Washington, D.C.: GAO, March 2003).

⁹⁹ *Ibid*, 50.

¹⁰⁰ *Ibid*, 44-49.

¹⁰¹ *Ibid*, 53-56.

research work.¹⁰² Of the 6,500 former biological and nuclear weapons scientists, 75 percent spent less than a third of their time on approved research projects, with no accounting for their other activities.¹⁰³ Meanwhile, the program has been essentially flat-funded at approximately \$50 million since fiscal year 2001.¹⁰⁴

SECURITY RECOMMENDATION

To address these shortcomings, funding for nonproliferation programs targeted at the former Soviet Union should be strengthened. Current funding, at approximately \$1 billion per year, is too low to secure or eliminate existing weapons of mass destruction, including biological weapons stockpiles, facilities, and capabilities. A tripling of current funding, to \$30 billion over the next 10 years, is required to secure all weapons of mass destruction sources and keep them out of the hands of terrorists.¹⁰⁵ A portion of these increases should be directed to identifying and securing bioweapons facilities from insider and outsider threats, as well as better tracking bioscientists' activities. Russian obstructionism in the effort to secure potential biological weapons is not acceptable. The Administration needs to increase pressure on Russian officials to cooperate and resolve disagreements blocking the achievement of security. Obtaining this cooperation must be a high priority in our dealings with Russia.

SECURITY GAP: There Are No International, Standardized Security Guidelines for Pathogen Research Sites and Collections.

Today, no comprehensive, uniform, global standards for laboratory security exist on which individual states can base national legislation and regulatory regimes.¹⁰⁶ Instead, potential bioweapons agents are stored in collections and laboratories in numerous countries, under varying degrees of security, and are exchanged through poorly monitored "germ commerce."¹⁰⁷ As a result, terrorist organizations could exploit poorly protected facilities or research material exchange systems, gain access to toxins and pathogens, and then use the material for bioterrorism on U.S. soil. The Administration has suggested that the World Health Organization (WHO) should take the lead in developing and communicating voluntary guidelines, and then wait for every nation to adopt regulations to meet these guidelines.¹⁰⁸ However, WHO is a public health and scientific organization, and it is not well equipped to deal with what is fundamentally a security issue. Moreover, such a process is likely to be slow, and fails to incorporate

¹⁰² GAO, *Weapons of Mass Destruction: State Department Oversight of Science Centers Program*, GAO-01-582, (Washington, D.C.: GAO, May 2001).

¹⁰³ Ibid, 18-19.

¹⁰⁴ Nuclear Threat Initiative, *Controlling Nuclear Warheads and Materials: Threat Reduction Budgets*, http://www.nti.org/e_research/cnwm/charts/cnm_funding_interactive.asp, visited February 13, 2004.

¹⁰⁵ U.S. Department of Energy, Secretary of Energy Advisory Board, *A Report Card on the Department of Energy's Nonproliferation Program's with Russia*, January 10, 2001.

¹⁰⁶ Jonathan B. Tucker, *Biosecurity: Limiting Terrorist Access to Deadly Pathogens*, Peaceworks No. 52 (Washington, D.C.: U.S. Institute of Peace, 2003).

¹⁰⁷ Jonathan B. Tucker, "In the Shadow of Anthrax: Strengthening the Biological Disarmament Regime" *The Nonproliferation Review*, (Spring 2002): 112; see also William J. Board, "Obtaining Anthrax Is Hard, But Not Impossible," *New York Times*, October 10, 2001, B12.

¹⁰⁸ Bureau of Arms Control, U.S. Department of State, *Security of Dangerous Pathogens and Toxins - Release from the August meeting of Experts to the Biological Weapons Convention*, August 25, 2003.

accountability, leaving a patchwork of inconsistently implemented and enforced regulations that could be exploited by terrorists.

SECURITY RECOMMENDATION

Having suffered from bioterrorism and as initiator of the world's largest biodefense research effort, the U.S. should provide leadership in the international arena to help secure dangerous agents that could be used as weapons in all countries. The Administration should reinvigorate multilateral negotiations towards developing effective and enforceable global controls on pathogen use, storage, and transfer.

SECURITY GAP: Efforts To Secure U.S. Pathogen Research Sites and Collections Have Been Inadequate.

In the U.S., stocks of dangerous pathogens, high-level laboratories to house them, and the number of people working with them are growing rapidly as efforts to improve the nation's biodefense expand. These reinvigorated efforts are essential to improving our biodefense, but they also bring more opportunities for the accidental or intentional escape of pathogens from legitimate facilities.¹⁰⁹

Congress mandated an increase in the security of inventories, laboratories, and personnel in the Bioterrorism Preparedness Act of 2002, establishing the "select agent" regulatory programs at the Centers for Disease Control and Prevention (CDC) and the U.S. Department of Agriculture (USDA).¹¹⁰ However, effective implementation of these security requirements has lagged. According to GAO, CDC suffered from "significant management weaknesses" that undermined administration of a relatively small regulatory program initiated before September 11.¹¹¹ Now, in charge of the much more expansive, post 9/11 requirements, the CDC, traditionally reluctant to manage a regulatory program, continues to struggle. Along with the Federal Bureau of Investigation and the USDA, the agency still has not met a deadline, originally set for November 12, 2003, for certifying the security of laboratories that use deadly pathogens.¹¹² The certification process requires facilities possessing dangerous agents to register with the government, and for the completion of a security risk assessment, implementation measures to ensure security, and the conduct of background checks on personnel with access to the agents. Instead of ensuring this security, the Administration has issued "provisional" certificates, with no timeline for final approval.

In the past, security at many research facilities has been weak. A USDA audit of more than 100 laboratories conducting publicly funded experiments on hazardous biological agents illustrated a number of security shortcomings, including a lack of security cameras and appropriate locks on

¹⁰⁹ Eileen Choffness, "Bioweapons: New Labs, More Terror?" *Bulletin of the Atomic Scientists*, 58, no. 5 (September/October 2002): 28-32.

¹¹⁰ Title II, *Public Health Security and Bioterrorism Preparedness and Response Act of 2002*, PL 107-188.

¹¹¹ GAO, *Homeland Security: CDC's Oversight of the Select Agent Program*, GAO-03-315R, (Washington, D.C.: GAO, November 2002).

¹¹² John Mintz, "U.S. Fails to Certify Many Labs that Use Pathogens," *The Washington Post*, November 12, 2003, A13.

doors and freezers, and poor or non-existent inventory records.¹¹³ Even though the federal government has spent more than \$3 billion in biodefense research and development over the last two years, verified safeguards at our own laboratories are woefully inadequate.

SECURITY RECOMMENDATION

The Administration should make it a high priority to fully implement the CDC and USDA select agent regulations mandated by Congress in order to secure pathogen stocks in this country. If these agencies do not take swift action, Congress should consider transferring responsibility for the “select agent” program to the Department of Homeland Security (DHS). While securing these laboratories must be done with appropriate balance so as to minimize the burden and uncertainty faced by researchers, our nation’s domestic security demands action instead of indefinite delay. In forging the cooperation and consistency between two separate cabinet-level agencies necessary for successful implementation of these security requirements, stronger leadership from the Administration appears necessary.

Effective Bioterrorism Preparedness for America

Preventing terrorist access to pathogens will reduce the risk of bioterrorism, but it cannot eliminate it. The recent anthrax and ricin attacks demonstrated that criminals already possess the ability to manufacture bioweapons. While terrorists can most easily acquire pathogens from existing stocks, many dangerous microbes and toxins can be extracted from natural sources as well. Finally, and most disturbingly, the knowledge and skill to bioengineer new, dangerous strains of pathogens and types of poisons is growing. According to an expert CIA panel, rapid advances in biotechnology are making possible the creation of biological agents that “could be worse than any disease known to man.”¹¹⁴ In the face of this evolving threat, effective bioterrorism preparedness is essential for homeland security, as it will save lives, calm the public, and, when achieved and demonstrated, deter bioterrorists.

SECURITY GAP: There is No Coherent or Comprehensive Biodefense Preparedness and Response Strategy.

A clear, overarching strategy is needed for biodefense preparedness and response, with well-defined and measurable goals for preparedness that are based on recognized threats and vulnerabilities. Without one, federal efforts risk being at best inscrutable, duplicative and wasteful, and, at worst, dangerously fragmented and uncoordinated. Unfortunately, the Administration has still not developed a coherent plan for biodefense preparedness and response, nor has it articulated an integrated, comprehensive strategy for building our biodefense. Federal cabinet agencies with responsibilities for bioterrorism preparedness and response include the Department of Homeland Security, the Department of Justice, the Department of Energy, the Department of Defense, the Department of Health and Human Services, the Department of

¹¹³ *Associated Press*, “Bioterror Concerns Raised at Universities,” November 21, 2003.

¹¹⁴ Office of Transnational Issues, Central Intelligence Agency, *The Darker Bioweapons Future*, OTI SF 2003-108, November 3, 2001, <http://www.fas.org/irp/cia/product/bw1103.pdf>.

Agriculture, and the Veterans Administration.¹¹⁵ These agencies must work with each other and, in turn, must coordinate with a plethora of state, local, and private institutions to develop standards and procedures for a coordinated preparedness and response to health crises. While a national strategy specifically addressing bioterrorism issues, *the National Strategy to Combat Weapons of Mass Destruction*, was released in December 2002, it is vague and does not clearly identify federal agency roles and responsibilities.¹¹⁶ While the Department of Health and Human Services (HHS) is required by law to complete a national preparedness plan for public health emergencies and report to Congress on its progress, as of the publication of this report, this exercise remains uncompleted and no progress report, first due in June of 2003, has been delivered.¹¹⁷ The current situation has led experts to identify a fundamental lack of coherent organizational systems, structures and chains of commands throughout the public and private biodefense infrastructure.¹¹⁸

Effective bioterrorism preparedness requires resources for planning and building detection and response capabilities. However, these resources will ultimately be wasted unless they are accompanied by a clear concept of bioterrorism preparedness and a strategy to achieve it. Clear and reasonable goals for public health and hospital preparedness, measured with quantitative and qualitative capacity and performance indicators, are essential. However, measures used to date have been insufficient. Meaningful standards are largely absent, and states continue to lack standards or guidance how to define preparedness, how to measure it, or how programs will be evaluated.^{119,120} The “critical benchmarks” applied to public health and hospital preparedness funding by HHS so far have been minimal in expectations and vague in direction, leaving states with the responsibility to define operational capacities and how to achieve them.¹²¹ The Administration has announced that DHS is now leading the effort to establish preparedness goals.¹²² However, no clear methodology or timeline for their delivery has been proposed. Meanwhile, CDC has begun its own new measurement initiative, called the Public Health Preparedness Project, intended to develop indicators to evaluate states’ preparedness.¹²³ But absent the context of a broader bioterrorism plan or a consensus on how measurable outcomes are linked to preparedness goals, it is unlikely that these indicators will have a sufficient real-world

¹¹⁵ James Jay Carafano, “Improving the Federal Response to Catastrophic Bioterrorist Attacks: The Next Steps,” *Heritage Foundation Backgrounder No. 1705*, November 15, 2003.

¹¹⁶ Raymond Decker, General Accounting Office, Testimony before the Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations, March 3, 2003 (GAO-03-519T).

¹¹⁷ Sec. 101 of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (P.L. 107-188), codified in 42 U.S.C. 300hh.

¹¹⁸ Chris Strohm, “Agencies Criticized For a Lack of Bioterrorism Strategy,” *Government Executive Magazine*, November 14, 2003, <http://www.govexec.com/dailyfed/1103/111403c1.htm>.

¹¹⁹ Bernard J. Turnock, *Public Health Preparedness at a Price: Illinois*, (New York, Century Foundation, 2003): 32.

¹²⁰ Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission), *Fourth Annual Report to the President and Congress*, December 2002, 54, <http://www.rand.org/nsrd/terrpanel/terror4.pdf>.

¹²¹ Bernard J. Turnock, *Public Health Preparedness at a Price: Illinois*, (New York: Century Foundation, 2003): 13, 22.

¹²² *Budget of the United States Government for Fiscal Year 2005, Analytical Perspectives*, (Washington, D.C.: GPO, 2004): 48.

¹²³ (a) CDC, *State and Local Preparedness-Progress in Achieving Critical Benchmarks*, presented by Joseph M. Henderson at the meeting of the HHS Secretary’s Council on Public Health Preparedness, Washington, D.C., January 22, 2004, <http://www.dhhs.gov/asphelp/presentation/040122presentationlist.html>; (b) Jonathan Radow, “CDC Develops Bioterror Scenarios to Evaluate Preparedness Indicators,” *Washington Fax*, November 19, 2003.

basis to accurately measure the many jurisdictions and capabilities needed for preparedness. In addition, financial accountability is generally poor. For example, CDC does not know what states are actually spending on public health or how federal funds are being spent, making it difficult to track activities within states or make comparisons between states.¹²⁴

Finally, in dealing with bioterrorism threats in particular, little consideration has been given to identifying or incorporating bioterrorism threats and vulnerabilities in the allocation of resources.¹²⁵ Instead, with the exception of four cities, grants to health agencies and hospitals are distributed in the same amount to all fifty states, with extra adjustments only on the basis of population.¹²⁶ As a result, Wyoming has received \$15 per capita in bioterrorism preparedness money, while Texas has received \$4. The evidence indicates a lack of a coherent strategy for public health preparedness or an working system to achieve it.

SECURITY RECOMMENDATION

The Administration should support the establishment of an Assistant Secretary for Bioterrorism and Public Health Emergencies at DHS. This single official would be responsible for the Department's bioterrorism-related efforts and facilitate coordination and cooperation with other agencies, particularly HHS.¹²⁷ In conjunction with HHS, this individual should spearhead the development of a comprehensive, cross-agency, multi-sector, national biodefense plan for preparedness and response and a strategy to achieve this state of readiness. The plan should clearly define the roles and responsibilities of each agency in each sector. Threat and vulnerability assessments need to be conducted and the results incorporated into preparedness and response planning. Such planning should also incorporate aspects unique to bioterrorism, such as forensic analysis. The plan should also seek to supply federal, state, local, and private institutions with the essential capabilities necessary to respond to bioterrorism and other public health emergencies. Those at the federal, state, and local level who are actually involved in the detection and response process must have input into defining these essential capabilities, and preparedness should be defined as their demonstrable achievement and maintenance.

Coherent metrics and goals should be developed so that progress towards preparedness can be achieved and measured. In addition to these metrics, a strategy for reaching these goals should be provided to guide federal, state, and local agencies, Congress, and our private sector partners in setting budgets and priorities. Intentional bioterrorism should not be the only focus. There are likely to be substantial "dual-use" benefits from an improved public health infrastructure that can be derived in numerous emergency situations, as well as day-to-day operations. Plans and standards that maximize these synergies should be developed.

¹²⁴ Shelly Hearne, President of Trust for America's Health, testimony before the House Committee on Government Reform, February 12, 2004.

¹²⁵ Council on Foreign Relations, *Emergency Responders: Drastically Underfunded, Dangerously Unprepared*, June 2003, 30-31.

¹²⁶ Holly Harvey, "Fiscal Year 2003 Funding Formula for Bioterrorism Grants," *Congressional Research Service Memorandum*, November, 2003.

¹²⁷ James J. Carafano, "Improving the Federal Response to Catastrophic Bioterrorist Attacks: The Next Steps," *Heritage Foundation Backgrounder*, no. 1705, November 13, 2003.

SECURITY GAP: Public Health and Hospital Preparedness Remain Weak.

While further planning and clear standards for preparedness are crucial, it is already evident that the nation's public-health and healthcare-delivery infrastructure, the frontline for bioterrorism detection and response, is in urgent need of better targeted, stronger, and sustained resources. Since 9/11, the Administration and Congress have directed approximately \$4 billion towards improving surveillance systems, communications, laboratory capacity, equipment, training, and other aspects of bioterrorism preparedness. However, it is becoming increasingly clear that these funds are poorly targeted and insufficient to meet more than the most modest preparedness goals.

According to Joseph Henderson, Associate Director for Terrorism Preparedness and Response at the CDC, neither "our public health system, nor any public health system in the world, is prepared for a significant bioterror event."¹²⁸ The problem, according to Mr. Henderson, is resources. "A billion seems like a lot, but we need more." Experts believe that the severe underfunding of the public health infrastructure over decades has left the system in desperate need of further overhaul,¹²⁹ and key services needed for bioterrorism preparedness, such as epidemiological capacity,¹³⁰ laboratory capacity,¹³¹ surge capacity,¹³² and communication and reporting systems,¹³³ remain weak. A December 2003 report by the nonpartisan Trust for America's Health found that at the state level, where preparedness programs are reportedly 100 percent financed by federal funds,¹³⁴ actual preparedness has only risen modestly and haphazardly.¹³⁵ State budget crises, delays in federal grants, and shortages of workers have left only six states with enough laboratory capacity to deal with a public health emergency, and only two with sufficient workers to distribute live-saving medicines from the Strategic National Stockpile. A GAO assessment of federal grants to state and local public health agencies and hospitals found no grantee has met all of the relatively modest "critical benchmarks" required in federal funding guidelines.¹³⁶ Local health agencies, those that will actually be involved in a response to bioterror attack, are being overlooked. The vast majority of these jurisdictions receive federal funding through state agencies. But they report delayed and insufficient allocations and poor collaboration with state planners.¹³⁷

¹²⁸ Caitlin Harrington, "Joe Henderson, CDC's Anti-Terrorism Chief, Gets Paid to Worry," *CQ-Homeland Security*, January 20, 2004.

¹²⁹ Committee on Assuring the Health of the Public in the 21st Century, Institute of Medicine, *The Future of the Public's Health in the 21st Century*, (Washington, D.C.: National Academy Press, 2003).

¹³⁰ "Terrorism Preparedness in State Health Departments – United States, 2001-2003," *Morbidity and Mortality Weekly Report*, 52, no. 43 (2003): 1051-1053.

¹³¹ Trust for America's Health, *Public Health Laboratories: Underprepared and Overwhelmed*, June 2003.

¹³² Victoria Elliott, "Public Health's Main Fear Over Bioterrorism: Surge Capacity," *American Medical News*, February 24, 2003.

¹³³ Institute of Medicine, *Microbial Threats to Health: Emergence, Detection, and Response*, (Washington, D.C.: National Academy Press, 2003).

¹³⁴ Elin Gursky, *Progress and Peril: Bioterrorism Preparedness Dollars and Health*, (New York: Century Foundation, 2003): 30.

¹³⁵ Trust for America's Health, *Ready or Not: Protecting the Public's Health in the Age of Bioterrorism*, December 2003.

¹³⁶ GAO, *HHS Bioterrorism Preparedness Programs: States Reported Progress but Fell Short of Program Goals for 2002*, GAO-04-360R, (Washington, D.C.: GAO, February 2004).

¹³⁷ (a) United States Conference of Mayors, *Second Mayors' Report to the Nation: Tracking Homeland Security Funds Sent to the 50 State Governments*, January 22, 2004, 19-20, http://www.mayors.org/72ndWinterMeeting/homelandreport_012204.pdf; (b) Elin Gursky, *Progress and Peril: Bioterrorism Preparedness Dollars and Health*, (New York: Century Foundation, 2003): 24-28.

Hospitals and frontline healthcare providers in particular remain underprepared. The GAO reported that no state was able to develop a plan to respond to an epidemic involving at least 500 persons. An independent task force on emergency responders determined that \$29.6 billion would be needed over the next five years to achieve adequate hospital preparedness.¹³⁸ However, at current fiscal year 2004 funding levels, it would take fifteen years to reach this target. Moreover, the Administration is moving in the opposite direction, requesting four percent and 11 percent reductions in fiscal year 2005 for hospital and public health preparedness funding, respectively. According to the Association of State and Territorial Health Officials, these proposed cuts could jeopardize state's ability to respond to a terror event, outbreak of infectious disease, or other public health threat or emergency.¹³⁹ In addition, the separate administration of hospital grants, which is funded through the Health Resources and Services Administration (HRSA) as opposed to CDC, is leading to the isolation of hospitals from other public health emergency planning and readiness.¹⁴⁰

SECURITY RECOMMENDATION

Funding for public health preparedness should be boosted. There is no evidence that the nation has achieved an adequate state of bioterrorism preparedness. Reducing this funding, as proposed by the Administration for fiscal year 2005, sends the wrong signal to state and local governments, indicating that federal funding to sustain readiness may be withdrawn in the future. This should be avoided as it will undermine our investments in preparedness.

The process for delivering federal funds to state and local jurisdiction needs reform. The Department of Health and Human Services should take greater advantage of its authority to provide more targeted funding directly to local or sub-state regional health agencies. Funding streams should be merged into a single Office of National Public Health Preparedness under the Assistant Secretary for Public Health Emergency Preparedness.

SECURITY GAP: The National Smallpox Vaccination Program Has Failed.

Smallpox is a deadly, disfiguring and contagious disease that could be devastating if used as a weapon by terrorists. While the virus that causes smallpox no longer exists in nature, there is reason to believe it may be accessible to terrorists. The huge Soviet biological weapons program produced tons of weaponized smallpox virus,¹⁴¹ and its former deputy director, Dr. Ken Alibek, is

¹³⁸ Council on Foreign Relations, *Emergency Responders: Drastically Underfunded, Dangerously Unprepared*, June, 2003: 35.

¹³⁹ Association of State and Territorial Health Officials, "ASTHO Says State Terrorism Preparedness Dollars Critical; Cuts in Proposed FY05 Budget Worrisome," press release, February 3, 2004, http://www.astho.org/templates/display_pub.php?u=JnB1YI9pZD0xMDEz.

¹⁴⁰ Bernard J. Turnock, *Public Health Preparedness at a Price: Illinois*, (New York: Century Foundation, 2003): 31-32.

¹⁴¹ (a) Ken Alibek, *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World*, (New York: Random House Inc., 1999); (b) *The 1971 Smallpox Epidemic in Aralsk, Kazakhstan, and the Soviet Biological Warfare Program*, Jonathan Tucker and Raymond Zilinskas, Eds., Chemical and Biological Weapons Nonproliferation Project, Monterey Institute of International Studies, Occasional Paper No. 9, July 2002.

certain that the virus has escaped from the Soviet program.¹⁴² Dr. D.A. Henderson, the former director of the world smallpox eradication effort, points out that the technology and expertise developed in the Soviet Union during the Cold War is now spread throughout the world.¹⁴³

To confront the threat, in 2002, the Administration directed states to develop smallpox preparedness programs. One of the goals was to vaccinate 500,000 healthcare workers and first responders during 2003 to provide an immune population who could, in turn, care for smallpox victims and administer vaccines to the general public in the event of an attack. Over one year later, a report by the Democratic Members of the Select Committee on Homeland Security has found that only 39,000 personnel have been vaccinated and states nationwide report indefinitely paused vaccination programs, inadequate preparedness, and no real-world means to measure progress or readiness in smallpox preparedness.¹⁴⁴ For example, Nevada reports only 17 vaccinated personnel, while Chicago and New York City have only one vaccinated health worker for every 40,000 people. Forty states report they are unable to vaccinate their populations within ten days of an outbreak. The Administration has contributed to the failure of the smallpox vaccination program through its poor leadership and mismanagement of the program's implementation. As a result, healthcare workers and the public at large have become complacent about the smallpox threat and resistant to vaccination, undermining confidence in the U.S. government and threatening the entire biodefense effort. According to Dr. Tara O' Toole, director of the University of Pittsburgh's Center for Biosecurity, smallpox preparedness has advanced "some small increment," but "essentially our readiness has not improved since 2001."¹⁴⁵

SECURITY RECOMMENDATION

The Administration should learn from the failures of the vaccination program and restart efforts to achieve smallpox preparedness. A new assessment of the smallpox threat should be made and communicated to state planners, first responders, and the public. Indicators of smallpox preparedness must be developed and integrated into preparedness plans. If these indicators show further vaccinations are required, a reinvigorated, fully funded vaccination effort should be initiated.

Protection Through New Medicines to Fight Pathogens

Truly effective preparedness for bioterrorism requires the tools to detect pathogens, prevent infection, and treat any who fall ill from exposure. According to a 2000 study by the Defense Science Board, at least 57 different countermeasures are needed to defend against 19 of the major bioterrorist agents. Today, only one countermeasure, antibiotic treatment for psittacosis, is

¹⁴² Ken Alibek. Testimony before the House Committee on Government Reform, Subcommittee on National Security, Veterans Affairs, and International Relations, October 12, 2001.

¹⁴³ David McGlinchey, "Smallpox Immunization Program Stalls," *National Journal*, November 7, 2003.

¹⁴⁴ Democratic Members of the House Select Committee on Homeland Security, *A Biodefense Failure: The National Smallpox Vaccination Program One Year Later*, January 2004, http://www.house.gov/hsc/democrats/pdf/press/040129_ABiodefenseFailureOneYearLater.pdf.

¹⁴⁵ Jonathan Rauch, "Smallpox is Bush's Worst Failure," *National Journal*, November 17, 2003.

effective through multiple disease stages and can be widely distributed.¹⁴⁶ Assessments by the National Institutes of Health have reached the conclusion that we lack many crucial means to defend against likely pathogens.¹⁴⁷ Existing anthrax and smallpox vaccines are too complex or hazardous to protect all population segments, and there are no FDA-approved drugs to treat those who become infected and ill. No vaccine exists for botulinum toxin, pneumonic plague, or tularemia, all considered potential bioterror weapons. Effective drug therapies for viral hemorrhagic fevers are few. In addition, first responders and hospital emergency rooms are without rapid diagnostic tools to detect anthrax, smallpox, plague, botulism, or tularemia.

It is increasingly difficult to separate the dangers of deliberate bioterrorism from those infectious disease threats that arise unintentionally, whether from globalization, environmental change, or evolutionary processes. This year's avian-flu virus in Asia appeared quickly and spread rapidly, putting the entire world on alert.¹⁴⁸ Severe acute respiratory syndrome (SARS), which has claimed more than 800 lives since its discovery, may have arisen from animal storage conditions in China, but spread rapidly overseas.¹⁴⁹ West-Nile virus, which has caused 403 deaths in the U.S. since 2002, and the mega-killer, AIDS, are diseases which traveled to this country from elsewhere. However, resistance of pathogens to existing drugs has become increasingly dangerous. Up to 75 percent of new AIDS patients in the U.S. are resistant to at least one existing antiretroviral therapy.¹⁵⁰ Between 1989 and 2001, some drug-resistant hospital bacterial infections doubled in the U.S.¹⁵¹ The national and homeland security implications of infectious disease have already been recognized. The National Intelligence Council concluded in 2000 that infectious diseases "will endanger U.S. citizens at home and abroad, threaten U.S. armed forces deployed overseas, and exacerbate social and political instability in key countries and regions in which the United States has significant interests."¹⁵² The nation will continue to face this threat as diseases evolve and new biological threats emerge.

SECURITY GAP: Project Bioshield Is Insufficient and Will Not Produce the Countermeasures We Need.

In proposing Project Bioshield, the Administration has recognized the need to build an arsenal of countermeasures against infectious disease. Today, private pharmaceutical and biotechnology firms are essentially the only entities with the capability to produce safe and effective vaccine,

¹⁴⁶ Defense Science Board, Department of Defense, "The Projected Evolution of Diagnostics, Vaccines, and Therapeutics Against Major Biogents with Strategic R&D and Supply Actions," *2000 Defense Science Board Summer Study*, (2000).

¹⁴⁷ (a) National Institutes of Allergies and Infectious Diseases, National Institutes of Health, *NIAID Biodefense Research Agenda for CDC Category A Agents*, publication no. 03-5308, February 2002; (b) National Institutes of Allergies and Infectious Diseases, National Institutes of Health, *NIAID Biodefense Research Agenda for CDC Category B and C Priority Pathogens*, publication no. 03-5315, January 2003.

¹⁴⁸ David Brown, "A Horror Script for Health Officials: Bird Flu Poses Global Epidemic Threat," *Washington Post*, January 25, 2004, A19.

¹⁴⁹ World Health Organization. *Summary of Probable SARS Cases with Illness Onset from 1 November 2002 to 31 July 2003*, (revised 26 September 2003), http://www.who.int/csr/sars/country/table2003_09_23/en/.

¹⁵⁰ R. Grant and others, "Time Trends in Primary HIV-1 Drug Resistance Among Recently Infected Persons," *Journal of the American Medical Association*, 288, no. 2 (2002):181-188.

¹⁵¹ Centers for Disease Control and Prevention, *MRSA-Methicillin Resistant Staphylococcus Aureas*. <http://www.cdc.gov/ncidod/hip/Aresist/mrsa.htm>.

¹⁵² National Intelligence Council, *National Intelligence Estimate: The Global Infectious Disease Threat and Its Implications for the United States*, NIE99-17D, (Washington, D.C.: NIC, 2000).

drugs, and medical diagnostics. Thus, the plan's key component, which seeks to engage the private sector in the development and manufacture of biodefense countermeasures, is a wise first step. However, as currently proposed, Bioshield still does not address critical weaknesses in both the government's and the private sector's ability to deliver biodefense technologies and, as a result, it is unlikely to produce the significant numbers of new medical products that are required for homeland security.

Project Bioshield's central provision, a purchase fund to provide a market for and thus stimulate development of biodefense countermeasures, is probably inadequate. The funding provided in the fiscal year 2004 Homeland Security Appropriations Act totals \$5.6 billion through 2014. However, as Rep. Harold Rogers (R-KY), chairman of the House Homeland Security Appropriation Subcommittee said, this amount is "chicken feed to this industry."¹⁵³ On average, the development of a new drug or vaccine takes up to ten years and costs \$900 million or more.¹⁵⁴ Based on the Defense Science Board's estimate of 56 needed countermeasures, Bioshield would only provide \$100 million per new product. This will not be enough to entice private sector firms away from much more lucrative markets in chronic disease treatment, obesity control, or "lifestyle conditions" such as baldness or sexual dysfunction. Medicines for these markets promise returns well above \$500 million per product over several years. These market realities have led to industry skepticism about Bioshield and calls for higher guaranteed profits, fewer restrictions on government contracts, and more favorable rules regarding ownership of new discoveries made under the program.¹⁵⁵

Compounding the reluctance of private sector companies to address this critical public health mission is the rapidly waning capability of pharmaceutical and biotechnology companies to produce the types of medicines needed for biodefense. Because of the potential for higher profits, most are abandoning antimicrobial products in favor of other, more long-term treatments.^{156,157} Since 1998, only seven new antibacterials have been approved, and of the 400 drugs likely to be approved in the near future, only five are antibacterial agents.¹⁵⁸ In addition, not a single new class of antibiotics is currently in development. Many generic, essential antibiotics are increasingly in short supply due to decreasing manufacturing capacity.¹⁵⁹ Antiviral drugs are also increasingly suffering from a loss of investment and limited development.¹⁶⁰ The situation with respect to vaccines is much worse. Industrial consolidations, the high cost of research and development (R&D), and persistent difficulties with maintaining profitability, have left the world

¹⁵³ *Bioshield: Countering the Bioterrorist Threat*, Hearing before the Select Committee on Homeland Security, U.S. House of Representatives, May 15, 2003.

¹⁵⁴ (a) Joseph A. DiMasi, Ronald W. Hansen, and Henry, G. Grabowski. "The Price of Innovation: New Estimates of Drug Development Costs." *Journal of Health Economics*, 22, no. 2 (2003):151-185; (b) Peter Landers, "Cost of Developing a New Drug Increases to About \$1.7 Billion" *Wall Street Journal*, December 8, 2003.

¹⁵⁵ Michael Barbaro, "Biodefense Plan Greeted With Caution," *Washington Post*, May 2, 2003, E1.

¹⁵⁶ Roxanne Nelson, "Antibiotic Development Pipeline Runs Dry," *The Lancet*, 362, no. 9397 (2003): 1726-1727.

¹⁵⁷ Tom Clarke, "Drug Companies Snub Antibiotics," *Nature*, 425, no. 6955 (2003): 225.

¹⁵⁸ Infectious Disease Society of America, *Bad Bugs, No Drugs: Defining the Antimicrobial Availability Problem*, Infectious Disease Society of America Backgrounder, November 2003, http://www.idsociety.org/Template.cfm?Section=Policy_and_Advocacy.

¹⁵⁹ Larry Strausbaugh, Daniel Jernigan, Laura Liedtke, "National Shortages of Antimicrobial Agents," *Clinical Infectious Diseases*, 33, no. 9 (2001):1495-1501.

¹⁶⁰ Institute of Medicine, *Microbial Threats to Health: Emergence, Detection, Response*, (Washington, D.C.: National Academy Press, 2003): 191.

with only five vaccine manufacturers and an anemic capability to develop new vaccines.¹⁶¹ According to the Institute of Medicine, “our nation and the world face a serious crisis with respect to vaccine development, production, and deployment.”¹⁶² Bioshield does not establish sufficient incentives or partnerships with the private sector to overcome these obstacles.

In recognition of the serious barriers to private sector involvement, the Administration has sought to build the federal capacity for countermeasures research and development at the National Institutes of Health (NIH). Since fiscal year 2003, the Administration requested and Congress appropriated more than \$3 billion for bioterrorism related R&D at NIH, mostly within the National Institute of Allergies and Infectious Diseases (NIAID). The Administration has requested another \$1.7 billion for fiscal year 2005. Project Bioshield also includes proposals that give NIH streamlined procurement, contracting, personnel, and peer-review authorities to enhance the institutes’ R&D capabilities. Some of these new powers and resources are to be devoted to basic research activities, a crucial investment and the traditional strength of NIH. The NIAID has also announced that it will devote much of its resources to developing and producing new medicines for biodefense.¹⁶³ However, as a recent Institute of Medicine report points out, “NIH has little tradition of product development.”¹⁶⁴ Instead, institutes at NIH have traditionally pursued basic research in order to enable private sector development and production of medical technologies. While these activities have provided remarkable advances in biomedical knowledge, NIH has not produced significant numbers of *specific* therapies. In fact, the later stages of clinical testing and product development have generally been left to case-by-case transitions arranged between NIH and the private sector. Of the hundreds of FDA-approved drugs and vaccines, NIH can count only 16 that have directly resulted from advances in its intramural research program.¹⁶⁵ In a separate analysis, NIH found that of a total of 47 FDA-approved “blockbuster” drugs, only four could be linked to government use or ownership rights to patented technologies.¹⁶⁶ Thus, despite recent claims of progress,¹⁶⁷ the history and traditional focus of NIH suggest that without more fundamental reform, the agency will be unlikely to produce the medicines necessary to counter the threat of bioterrorism.

¹⁶¹ Institute of Medicine, *Financing Vaccines in the 21st Century: Assuring Access and Availability*, (Washington, D.C.: National Academy Press, 2003): 107-144.

¹⁶² Institute of Medicine, *Microbial Threats to Health: Emergence, Detection, Response*, (Washington, D.C.: National Academy Press, 2003): 189.

¹⁶³ Anthony Fauci, “Biodefense on the Research Agenda,” *Nature*, 421, no. 6924 (2003): 787.

¹⁶⁴ Institute of Medicine and National Research Council, *Giving Full Measure to Countermeasures*, (Washington, D.C.: National Academies Press, 2004): 54.

¹⁶⁵ Office of Technology Transfer, NIH, *FDA Approved Therapeutic Drugs and Vaccines Developed with Technologies from the Intramural Research Program at the National Institutes of Health as of April 1, 2003*, <http://ott.od.nih.gov/NewPages/therapeutics.pdf>.

¹⁶⁶ National Institutes of Health. *A Plan to Ensure Taxpayers' Interests are Protected*, July, 2001, <http://www.nih.gov/news/070101wyden.htm#execsum>.

¹⁶⁷ National Institutes of Allergies and Infectious Diseases, *NIAID Biodefense Research Agenda for CDC Category A Agents: Progress Report*, August 2003, http://www.niaid.nih.gov/biodefense/research/category_A_Progress_Report.pdf.

SECURITY RECOMMENDATION

The Administration should work with Congress to move beyond Bioshield and develop and implement a strategy that will succeed in producing the safe and effective medical countermeasures we need. Only by working with the private sector and closely following successful medical product development models can government leverage these capabilities to produce the drugs, vaccines, and diagnostics needed to confront bioterrorism and other infectious disease threats. The Administration should establish new, much more innovative mechanisms, such as federally funded venture capital and “virtual” drug development firms, to develop and utilize the best public, private, and academic scientific and technological capabilities to counter microbial threats.

SECURITY GAP: The Threat of Unknown, Resistant or Bioengineered Pathogens Remains Unaddressed.

The Administration has not articulated a vision or developed a plan to confront the new, unexpected infectious disease or bioterrorism threats we will face for years to come. As noted above, the ongoing revolution in the life sciences could propel bioweapons development into a new era of sophistication, enabling the engineering of agents capable of overcoming existing countermeasures.¹⁶⁸ At the same time, our ability to confront certain infectious diseases remains poor. The most recent influenza season was worsened by the failure of current technology to produce sufficient quantities of vaccine for all of those who needed it or to provide the vaccine targeted to combat the actual observed strain.¹⁶⁹ A year after the emergence of SARS, we remain without an effective treatment or vaccine. These kinds of threats can be confronted with broad-spectrum antimicrobial and immunoprotective strategies, as well as the means to rapidly detect, analyze and produce more specific treatments against new, unexpected pathogens. However, only a few, small federal programs exist in these areas, and they remain uncoordinated.¹⁷⁰ In particular, designing and producing new medicines very rapidly - ideally, in a matter of weeks or months under emergency conditions - is a capability that will benefit homeland security as well as other aspects of healthcare. As noted above, the process of moving from “bug-to-drug” can take more than ten years and cost more than \$900 million. It should be possible to reduce this timeframe. In fact, the Defense Science Board has outlined a program for meeting this goal by taking advantage of modern proteomics and genomics, better molecular targeting technologies, advances in high-throughput techniques, and computational optimization of drug candidates.¹⁷¹ So far, these recommendations have not resulted in specific policy proposals.

¹⁶⁸ Bradley A. Smith, Thomas V. Inglesby, and Tara O'Toole, “Biodefense R&D: Anticipating Future Threats, Establishing a Strategic Environment,” *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, 1, no. 3 (2003): 193-202.

¹⁶⁹ Lawrence Altman, “The Big Bad Flu, or Just the Usual,” *New York Times*, December 14, 2003, A43.

¹⁷⁰ For example, see Defense Advanced Research Projects Agency, Department of Defense, *Pathogen Countermeasures*, <http://www.darpa.mil/dso/thrust/biosci/upathcm.htm>.

¹⁷¹ Defense Science Board, Department of Defense, *2001 Summer Study on Defense Science and Technology*, (May 2002): 108-115, <http://www.acq.osd.mil/dsb/sandt.pdf>.

SECURITY RECOMMENDATION

The Administration should explore the feasibility of a broad multi-agency effort to dramatically improve the “bug-to-drug” response time. Compressing the timeline for drug and vaccine development is a critical element of facing future bioterrorist and infectious disease threats. Achieving this transformation will not be easy, and it will require the participation and cooperation of many federal agencies and the private sector. It is an endeavor worthy of American ingenuity and leadership, and it will be as challenging as it will be beneficial, for biodefense, public health, and the economy.

**PROTECTING OUR BORDERS
ON SEA, LAND, & AIR**

Securing Our Ports

America's seaports remain vulnerable to terrorist attacks. Terrorists could cause mass casualties and serious damage to the economy if a weapon of mass destruction (WMD) is detonated in a container or if a large passenger vessel is attacked. The Department of Homeland Security has several initiatives dedicated to preventing terrorists from attacking America's ports. Despite these efforts, many security gaps remain. Container shipments are not secure from their points of origin to their final destination, and many ports are struggling to make physical security improvements. To remedy these problems, the Administration should improve the integrity of container shipments, develop a credible system of inspection and make sufficient resources available to local ports for security enhancements.

America's maritime transportation system is the gateway to the global economy. Our country's economic prosperity rests on the ability of tons of containerized cargo arriving unimpeded at U.S. ports to support the "just-in-time" delivery system, that underpins our manufacturing and retailing sectors. A majority of America's energy sources arrive in large oil and gas tankers. America's ports and waterways are also used to carry millions of citizens on cruise ships and ferries. While the transportation system is incredibly efficient, as port security expert Stephen Flynn states "it was built without credible safeguards to prevent it from being exploited or targeted by terrorists or criminals."¹⁷² An attack in a port could result in a substantial loss of life and an economic damage ranging from \$58 billion to \$1 trillion.¹⁷³

There are many vulnerabilities within the maritime transportation system. The high volume of containers and their efficient movement from foreign ports to the U.S. make container shipments a prime target for terrorist activity. Cargo containers could be used to smuggle terrorists or dangerous materials into the U.S. or as the delivery vehicle for a weapon of mass destruction. The Intelligence Community has warned that the United States is more likely to be attacked with a weapon of mass destruction delivered by ship, truck, or airplane than by a ballistic missile.¹⁷⁴ Large fuel tankers, cruise ships, and ferries are vulnerable to a variety of threats ranging from an explosive device being placed on board or small boat attacks similar to those on the *USS Cole* or French tanker *Limberg*. Such attacks could have significant fatalities, cause serious environmental damage, or potentially block the entranceway to a harbor, bringing local commerce to a halt. The Interagency Commission on Crime and Security at Seaports concluded just prior to 9/11 that security at U.S. ports "generally ranges from poor to fair and in few cases good."¹⁷⁵

¹⁷² Council on Foreign Relations, Testimony of CDR Stephen Flynn, USCG (ret), Jeane J. Kirkpatrick Senior Fellow in National Security Studies, *The Fragile State of Container Security*, Stephen Flynn, before the Committee on Governmental Affairs, United States Senate, Stephen Flynn (Washington D.C.: March 20, 2003)

¹⁷³ \$58 billion estimate is from the *Port Security Wargame-Implications from the Supply Chain*, Booz-Allen-Hamilton. February 2003. www.boozallenhamilton.com. \$1 trillion comes from Michael O' Hanlon, *Protecting the American Homeland*, (Washington D.C.: The Brookings Institute Press 2002.)

¹⁷⁴ U.S. National Intelligence Council, *Foreign Missile Developments and the Ballistic Missile Threat Through 2015*, December 2001. www.cia.gov/nic/other_missilethreat2001.html

¹⁷⁵ Interagency Commission on Crime and Security at U.S. Seaports, Fall 2000, 5.

Container Security

Improving container security is a major challenge. Individual containers must be made less vulnerable to tampering, and companies must strengthen the security of their supply chains. Finally, the inspections process must be made more vigorous without imposing an undue burden on the flow of commerce.

SECURITY GAP: Cargo Containers Are Vulnerable to Tampering.

One of the major vulnerabilities of container shipments is the lack of physical security of containers as they transit through the supply chain. The physical security of containers has long been a problem as criminals have easily broken into them to steal cargo and smuggle contraband. According to a recent RAND report on container security, there are no minimum security standards for containers.¹⁷⁶ The majority of containers are sealed with a lead tag which does not prevent access into a container. In addition, criminals break into containers without disturbing the seals such as cutting into the side or removing the doors.¹⁷⁷ According to RAND, an experienced thief can break into a sealed container in twenty minutes without disturbing the seals.¹⁷⁸

The Administration has undertaken a series of efforts to address the problem through initiatives such as Operation Safe Commerce and the Smart Box Initiative. Operation Safe Commerce is a demonstration program managed by the Transportation Security Agency (TSA) that has attempted to identify technology to secure containers such as electronic seals that signal an alarm if tampering occurs. It will expire at the end of fiscal year 2004. The Smart Box Initiative is a Customs and Border Protection (CBP) program, in which aims to reward companies that seal containers with a security seal and place sensors inside their containers by reducing the likelihood these containers would be delayed in the inspection process. While these efforts are admirable, the end result is that DHS still has not developed minimum standards for sealing containers. Rather, DHS has recently announced that it will be working with industry over the next six months to develop "recommendations" for sealing requirements. Thus for the foreseeable future, millions of containers will continue arriving in the U.S. sealed with tags that are not tamperproof.

In addition to the physical security weaknesses of containers, there is no process for verifying that containers remain sealed as they move through the supply chain. A container moves through many port terminals between the time it is loaded at a warehouse and when it reaches its final destination. This gives terrorists many opportunities to break into a container, plant a weapon of mass destruction inside and reseal it without anyone checking to see if the container has been opened until it reaches a U.S. port.

¹⁷⁶ Voort, Maarten van de, Kevin O'Brien, Adman Rahman, and Lorenzo Valeri. *Seacurity: Improving the Security of the Global Sea-Container Shipping System*, (RAND) August 12, 2003, 9.

¹⁷⁷ Council on Foreign Relations, Testimony of CDR Stephen Flynn, USCG (ret), Jeane J. Kirkpatrick Senior Fellow in National Security Studies, *The Fragile State of Container Security*, Stephen Flynn, before the Committee on Governmental Affairs, United States Senate, Stephen Flynn (Washington D.C.: March 20, 2003)

¹⁷⁸ Voort, Maarten van de, Kevin O'Brien, Adman Rahman, and Lorenzo Valeri. *Seacurity: Improving the Security of the Global Sea-Container Shipping System*, (RAND) August 12, 2003, 9.

SECURITY RECOMMENDATION

Container integrity can be enhanced through the adoption of minimum standards for container seals and the development of a seal verification process. DHS, at a minimum, should require all shippers to seal containers with the high security seal approved by the International Standards Organization. This is an electronic or mechanical seal that has unique markings and easily shows signs of tampering compared to lead tags seals currently in use. DHS also should develop a chain of custody for containers, requiring the verification of seals at the major stages of the supply chain such as when a container is loaded, or when placed on a vessel, train, or truck. Radio Frequency Identification technology can play a helpful role in verifying the status of seals.

SECURITY GAP: Containers Traveling Through the Supply Chain Are Vulnerable.

Containers are very susceptible to terrorist exploitation as they move through the supply chain. Many foreign warehouses do not have solid security controls including criminal background checks on personnel. The transit between the warehouse and foreign departure ports is believed to highly vulnerable, as containers carried on trucks and trains sit unguarded in parking lots, loading docks, and rail yards. While security at most foreign ports is a better than security at warehouses, many foreign ports have not yet taken the steps to improve their security in accordance with the International Maritime Organization port security requirements.¹⁷⁹ Containers placed on ocean carriers may not be sealed or checked for tampering. Once a container vessel arrives in the U.S., it is loaded on a truck or train and taken to its final destination. During this phase the whereabouts of the cargo are unknown, creating a vulnerability similar to the transit between the warehouse and foreign port.

The DHS developed the Customs Trade Partnership Against Terrorism (C-TPAT) to strengthen supply chain security. Launched in November 2001, C-TPAT is a government-business initiative between CBP and industry designed to improve security by having companies volunteer to sign agreements committing them to implementing a set of security practices in their supply chain. In return, participating companies have their score in CBP's Automated Targeting System (ATS) lowered, reducing the likelihood their shipments will be inspected. DHS officials have boasted about the success of C-TPAT. In October 2003, CBP Commissioner Robert Bonner stated that "C-TPAT is the largest and most successful government-private sector partnership to emerge from the ashes of 9-11."¹⁸⁰

C-TPAT is a useful first step in encouraging the private sector in being pro-active about supply chain security. However, C-TPAT's potential is being compromised by CBP's limited resources to process the applications of 5,300 companies and to conduct on-site verification of the

¹⁷⁹ Mark Huband, "Terrorist Threat to Shipping Still High as Authorities Slow to Implement Security Code," *Financial Times*, November 17, 2003, 13. The International Maritime Organization develop The International Ship and Port Facility Security (ISPS) code in December 2002. 163 nations included the US are signatories.

¹⁸⁰ U.S. Bureau of Customs and Border Protection, Remarks by Commissioner Robert Bonner, C-TPAT Conference, October 30, 2003.

http://www.cbp.gov/xp/cgov/newsroom/commissioner/speeches_statements/oct302003.xml

companies' security practices.¹⁸¹ According to Stephen Flynn, the major weakness in C-TPAT is "the nearly complete absence of Customs personnel to monitor the level of compliance among C-TPAT participants."¹⁸² Although CPB is currently conducting validations, it does not have enough personnel to complete them within the next year. This fact is troubling in light of the threefold increase in C-TPAT membership over the last year. As of January 2004, only 130 C-TPAT members had been verified leaving thousands of companies receiving a benefit of reduced inspections without any assurance that security has actually improved.¹⁸³ CBP requested an additional \$15.2 million in its fiscal year 2005 budget to hire 120 supply chain specialists to conduct validations. These positions will be combined with new personnel expected to be hired in 2004 as a result of resources previously provided by Congress. However, given the growth of the program such resources may not be sufficient to ensure that all companies can have their security practices validated within the next year. CBP also does not have a plan to audit C-TPAT members at a regular interval after they have received initial validation or conduct random inspections to ensure they comply with C-TPAT guidelines. Another weakness, according to RAND, is that C-TPAT does not address the land transit of containers to foreign debarkation ports, which it describes as the "most vulnerable phase in a container's transport."¹⁸⁴

SECURITY RECOMMENDATION

CPB should improve its ability to validate C-TPAT companies to ensure they are not receiving the benefit of reduced inspections without meeting their security responsibilities. CBP should strive to complete the validations within the next year. One possible solution is a partnership with reputable private companies to conduct the on-site verifications. These private companies would model the classification societies used in marine safety which are recognized by the U.S. Coast Guard to ensure vessels comply with international safety standards. These companies would be subject to CBP oversight. An annual audit plan should be developed to ensure that companies' security practices are checked beyond the final validation. CBP should establish "red teams" to test security compliance beyond announced examinations and determine whether C-TPAT security measures are sound.

¹⁸¹ Bureau of Customs and Border Protection, Testimony of Robert Jacksta, Executive Director Border Security and Facilitation Office of Field Operations, Before Committee on the Judiciary, United States Senate, January 27, 2004.

¹⁸² Council on Foreign Relations, Testimony of CDR Stephen Flynn, USCG (ret), Jeane J. Kirkpatrick Senior Fellow in National Security Studies, *The Fragile State of Container Security*, Stephen Flynn, before the Committee on Governmental Affairs, United States Senate, Stephen Flynn (Washington D.C.: March 20, 2003)

¹⁸³ Bureau of Customs and Border Protection, Testimony of Commissioner Robert Bonner, Before the National Commission on Terrorist Attacks Upon the United States. January 26, 2004.
http://www.cbp.gov/xp/cgov/newsroom/commissioner/speeches_statements/jan262004.xml

¹⁸⁴ Voort, Maarten van de, Kevin O'Brien, Adman Rahman, and Lorenzo Valeri. *Seacurity: Improving the Security of the Global Sea-Container Shipping System*, (RAND) August 12, 2003, 4.

SECURITY GAP: Container Inspections Are Not Sufficiently Comprehensive To Detect or Deter Attacks.

Recognizing that a nuclear weapon smuggled in a cargo container is one of the most significant threat facing America, DHS has attempted to improve the process used to inspect cargo. Prior to 9/11, the former Customs Service inspected two percent of all cargo containers by physically opening them to verify the contents. After 9/11, security officials acknowledged that the threat of chemical, biological or nuclear weapons being smuggled into the U.S. in a container required such containers to receive greater scrutiny. However, with more than seven million containers arriving at U.S. seaports annually, government officials realized that physically searching 100 percent of containers would be impractical and would severely slow down the flow of commerce. In response, DHS developed a risk management approach to identify high risk containers that warrant further scrutiny. CBP has created a cargo targeting center, required freight manifest information be submitted 24-hours prior to loading, assigned inspectors overseas, required the inspection of all high risk containers and placed some non-intrusive inspection equipment at U.S. seaports.

Such efforts, however, are not sufficient to ensure that the current inspection regime is an effective deterrent. Even with the previously mentioned improvements, CBP still inspects, either through physical inspection or some technological screening, only five percent of inbound containers. Furthermore, a technical recent report completed by Professor Lawrence Wein of Stanford University and Stephen Flynn concluded that current inspection practices have a only ten percent likelihood of detecting the most significant threat, a shielded nuclear weapon smuggled in a container.¹⁸⁵

- **Targeting Efforts Require Improvement to Determine Which Containers Pose a Risk.**

The National Targeting Center (NTC) is an operation center that is run by CBP responsible for reviewing manifest data in the ATS to determine which container shipments should be inspected. The NTC sets the anti-terrorism parameters for ATS and sends targeting information to inspectors at foreign and U.S. seaports. CBP also has manifest review units that are responsible for targeting containers headed to U.S. ports. The NTC's efforts are helped by the 24-hour rule, which requires carriers to send CBP manifest data 24 hours before a container is loaded on a vessel. The rule also requires specific information about the cargo which is an improvement over the vague cargo descriptions provided by shippers before 9/11.

Even with these improvements container targeting is flawed. The major weakness is that the data used by the NTC and CBP inspectors primarily comes from cargo manifests. According to GAO testimony on targeting, manifests are recognized by terrorism experts, the trade community, and CBP inspectors to be unreliable documents for targeting purposes.¹⁸⁶ If the data inputted into ATS is flawed, then the risk assessment of a container is unreliable and the entire container inspection system is suspect. Another problem with CBP targeting is that shippers are allowed

¹⁸⁵ Lawrence Wein, Alex Wilkins, Manas Baveja, and Stephen Flynn, *Preventing the Importation of Illicit Nuclear Materials in Shipping Containers*. November 4, 2003.

¹⁸⁶ Richard Stanna, *Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers*. U.S. General Accounting Office. Testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives. December 16, 2003, 11.

revise manifests sixty days after a container arrives. According to GAO, one-third of the manifest revisions resulted in a higher ATS score, but by the time the revisions were discovered, the cargo often was inside the U.S. after having been released from its arrival port.¹⁸⁷

SECURITY RECOMMENDATION

CBP must strengthen its targeting system by requiring the submission additional trade information which includes a more specific description of the cargo verified by the exporter and reduce the time period in which information on a manifest can be changed. DHS should develop a system to share threat and vulnerability information with all of the industries in the supply chain. This system could exist in the form of an Information Sharing and Analysis Center (ISAC) used in other industries. Ports, carriers, and shippers could report on security lapses in the supply chain to the ISAC and in return would have access to unclassified maritime threat and security information such as piracy incidents. This system would greatly help CBP's targeting efforts because it will give targeting personnel specific information on supply chain security breakdowns which does not exist in trade data.

- **Cargo Containers Are Not Comprehensively Screened For Weapons of Mass Destruction.**

According to CBP, it is addressing the weapons of mass destruction threat by deploying non-intrusive inspection devices such as radiation pagers, handheld isotope identifiers and Vehicle and Cargo inspection (VACIS) machines at seaports. Despite CBP Commissioner Bonner's continued statement that radiation pagers are "an important tool to detect radioactive materials moving through a port" the radiation pagers are a safety device that alarm inspectors of the presence of radiation.¹⁸⁸ Officials at the Department of Energy have stated that the pagers are not search instruments and are not designed to detect weapons usable nuclear material such as enriched uranium.¹⁸⁹ The handheld isotope identifiers can identify the type of radiological or nuclear material that may be in a container, but are primarily used as a secondary inspection device. VACIS is primarily an x-ray machine, providing an image of the contents inside a container but these machines are not capable of detecting radiological or nuclear material. In addition, many ports only have one VACIS machine, which is insufficient to screen all high risk containers at many seaports. CBP did not request any additional VACIS machines for domestic ports in its fiscal year 2005 budget.

Radiation portal monitors are the non-intrusive detection devices most capable of detecting nuclear and radiological material. The other great advantage of radiation portals is they can be fully integrated into port operations, which means that containers can be run through a portal by truck and rail without slowing the movement of commerce. Thus, not only are these portals far

¹⁸⁷ Ibid.

¹⁸⁸ Bureau of Customs and Border Protection, Testimony of Commissioner Robert Bonner, Before the National Commission on Terrorist Attacks Upon the United States. January 26, 2004.
http://www.cbp.gov/xp/cgov/newsroom/commissioner/speeches_statements/jan262004.xml

¹⁸⁹ Gary L. Jones, *Customs Service: Acquisition and Deployment of Radiation Detection Equipment*. U.S. General Accounting Office. Testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives. October 17, 2002.

superior to pagers and VACIS machines for the purpose of identifying dangerous materials, but they can also be used to screen 100 percent of the containers that enter U.S. ports. Using radiation portals is far more reliable way to prevent weapons of mass destruction from entering the United States than the labor intensive and somewhat unreliable method of targeting and physically inspecting only high risk containers. As Flynn and Wein noted, the integration of non-intrusive inspection devices into the supply chain could improve the trade off between cost and security due to “low equipment and labor cost of passive testing, the simplified logistics of testing at the gates, and the automated nature of passive testing.”¹⁹⁰

CBP plans to deploy portals at major points of entry including the twenty-two major seaports which handle ninety percent of inbound containerized cargo. According to agency officials, CBP has received the funding for portals at seaports, however this installation will be completed in March 2005 at the earliest. Currently, the Port of Norfolk is the only seaport in the nation with fully operational portal monitors at its major terminals. These portals were installed at the port’s expense. The portals are located at various chokepoints ensuring every container which leaves the port by truck or train is screened for nuclear or radiological material.¹⁹¹ Yet, according to port authority officials, the portals are integrated into daily operations and do not slow commerce.

SECURITY RECOMMENDATION

CBP should accelerate the installation of radiation detection portals and increase the number of VACIS machines at seaports to have an efficient and effective inspection process. DHS must begin to look at ways to better integrate the inspection process into supply chain operations. Efforts like those undertaken at the Port of Norfolk should be used as a model to determine ways to strengthen the inspection process without slowing the movement of goods. CBP should also invest in developing a device that combines the attributes of a radiation portal monitor and VACIS machine for the purpose of identifying a well hidden nuclear weapon in a cargo container.

In addition, VACIS machines should connect to an analysis center at which inspectors would review VACIS images and the images would be stored in a database. This center at would provide two benefits. First, it will allow VACIS images to be transmitted between ports, so if a container is screened at a CSI port overseas, the image could be sent to the domestic port where it contents could be re-examined. Second, an image database could also increase the effectiveness of VACIS inspections because inspectors would have files of images to reference.

- **Robust Inspections Require More Inspectors.**

Even as non-intrusive inspections are gradually integrated into port operations, CBP inspection programs will not be effective without significant personnel increases. Currently, DHS domestic and foreign container inspection operations do not have enough personnel to conduct vigorous cargo inspections. One such program is the Container Security Initiative (CSI). CSI sends inspectors overseas to inspect containers at the point of origin. DHS has reached agreements with 19 of the 20 “megaport” nations to allow CSI teams to operate. Megaports are the world’s twenty largest ports by volume and handle roughly seventy percent of U.S.-bound cargo. CPB currently deploys five-person teams to CSI ports with the exception of some of the larger ports which have

¹⁹⁰ Lawrence Wein, Alex Wilkins, Manas Baveja, and Stephen Flynn, *Preventing the Importation of Illicit Nuclear Materials in Shipping Containers*. November 4, 2003.

¹⁹¹ House Select Committee on Homeland Security staff trip to Norfolk, VA November 20, 2003.

two to three additional team members. The team consists of a research analyst, a special agent, and three inspectors. Currently 17 teams are fully operational.

While CSI is a very worthy effort, the current personnel levels are too low. Stephen Flynn has stated that CSI would require “the equivalent of a diplomatic service” to be an effective deterrent. One five person team deployed to a megaport is inadequate. The five-person team in Singapore, which sent more than 400,000 containers to the U.S. from March 2003 to January 2004, reviewed only sixty-three percent of cargo manifests.¹⁹² This means 160,000 manifest were not even reviewed to determine the risk of the cargo. Additionally, the GAO has reported that under the CSI program inspectors are only temporarily stationed overseas for 120 days.¹⁹³ Sending inspectors overseas for such a short period of time is not sufficient to ensure that they develop the relationships with foreign customs services necessary to obtain the information required to effectively target shipments. CBP has plans to expand CSI beyond the 20 megaports to cover 20 – 25 additional strategic ports around the world. However, under this plan, ports in high-risk countries such as Pakistan and Indonesia would not be covered. Moreover, the GAO has reported that CBP has no long term staffing plan to support the expansion of CSI to additional ports. The fiscal year 2005 budget includes funding to provide 98 additional CSI inspectors, however, given the expansion of CSI more resources may be needed to ensure cargo at foreign ports receive sufficient scrutiny before it is shipped to the U.S.

Inspection resources at U.S. ports are also stretched thin and will need to increase. According to a 2002 House Government Reform Committee report, the Port of New York/New Jersey had 64 inspectors dedicated to inspecting incoming cargo at a port which handles an average of one million inbound containers a year.¹⁹⁴ The report stated that the former Customs Service had 899 of its nearly 7,600 inspectors dedicated to seaports. To support CSI, CBP sends inspectors overseas for three to four months leaving U.S. ports short of inspectors. While ports have received additional inspectors, more will be needed to support the enhanced domestic and foreign inspection operations occurring since 9/11. For example, according to the GAO, CBP protocols call for random inspections of containers, even if they have not been identified as high-risk.¹⁹⁵ Before 9/11 inspectors would randomly examine containers to ensure the information on the manifest matched the contents of the container. However, CBP is not conducting random inspections at many ports because they only have enough inspectors to inspect only high risk cargo. This is the case in one major seaport, where random inspections have not been performed since 9/11 due to personnel constraints.¹⁹⁶

¹⁹² Weekly Statistics from CSI Singapore.

¹⁹³ ¹⁹³ *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors* U.S. General Accounting Office, GAO-03-770. July 2003, 12.

¹⁹⁴ *Federal Law Enforcement at The Borders and Ports of Entry* Report of the Subcommittee on Criminal Justice, Drug Policy and Human Resources, 80. July 2002.

¹⁹⁵ Richard Stanna, *Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers*. U.S. General Accounting Office. Testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives. December 16, 2003, 11.

¹⁹⁶ Democratic Staff visit August 28-29, 2003.

SECURITY RECOMMENDATION

Customs and Border Protection should develop a human capital plan to determine the number of inspectors required to support CSI assignments of at least one year and increase cargo inspections at U.S. seaports.

Port Security

Seaports present terrorists with an attractive target because they are large, open facilities, readily accessible by water and land, often located in metropolitan areas, and interwoven with other transportation systems and critical infrastructure. The GAO has concluded that the large amount of high value cargo, hazardous materials, and people moving through ports at a given time make ports potential terrorist targets.¹⁹⁷ These factors led the FBI Assistant Director for Counterterrorism to state that ports are “inherently vulnerable” to terrorist attacks.¹⁹⁸ Similarly, Secretary of Homeland Security Tom Ridge stated that “The protection of our ports -- and the thousands of cargo containers that flow through them each day -- is a critical focus area of homeland security.”¹⁹⁹ Congress acted to reduce ports vulnerability by passing the Maritime Transportation Security Act (MTSA) which President Bush signed on November 25, 2002.

SECURITY GAP: DHS Should Move Faster To Implement The Maritime Transportation Security Act.

The MTSA requires numerous measures designed to improve port security, including facility and vessel security plans, transportation identification cards, Coast Guard maritime security teams and vessel identification systems. While DHS has moved to implement certain provisions in the law, many important provisions have not been put into place. The Coast Guard has required ports and vessels to develop security plans, has brought seven Maritime Safety and Security Teams (MSST) online, and issued regulations requiring that vessels install identification systems. DHS has also begun to develop the Transportation Worker Identification Card (TWIC) with pilot projects in the ports of Philadelphia and Los Angeles/Long Beach.

However, DHS must begin to address other crucial MTSA sections such as the National Maritime Transportation Security Plan, foreign port security assessments, and a long range vessel tracking system.²⁰⁰ The MTSA requires the Secretary of Homeland Security to prepare a national plan that coordinates the efforts at the federal level to prevent and respond to a terrorist attack at a port. The plan must include the assignment of responsibilities among federal agencies, and a surveillance system designed to ensure that threats to the maritime sector are identified and reported to appropriate federal and state agencies. The plan also requires that the flow of cargo through U.S. ports is reestablished as efficiently and quickly as possible in the event of a terrorist attack which would minimize the economic damage associated with an attack on a port. Additionally, the law requires the Secretary of Homeland Security to assess security at foreign

¹⁹⁷ *Port Security: Nation Faces Formidable Challenges in Making Initiatives Successful*. US General Accounting Office, JayEtta Z. Hacker, GAO-02-993T, August 5, 2003.

¹⁹⁸ Testimony of Gary Ball, Acting Assistant Director for Counterterrorism, Federal Bureau of Investigation before the Senate Judiciary Committee, January 27, 2004.

¹⁹⁹ Remarks on port security from Secretary Tom Ridge, June 12, 2003. www.dhs.gov

²⁰⁰ Maritime Transportation Security Act, Sections 70103, 70108, and 70115.

ports and gives the Secretary the option of developing a long range vessel tracking system. This system would use satellite technology to track and monitor vessels to determine if they are threats and would give the Coast Guard the ability to intercept vessels before they reach an American port. At this time, there is no plan to re-route cargo in the event of a terrorist attack on a port, no plan on how the security at foreign ports will be assessed, or movement towards the development of a long range vessel tracking system.

SECURITY RECOMMENDATION

DHS should move faster to develop the National Maritime Transportation Security Plan to ensure coordination in the prevention and response to attacks or alerts and that economic damage is minimized by the efficient re-routing of cargo. DHS must also create a plan on how it will assess the security at foreign seaports and what the recourse will be if security gaps are discovered. If DHS wants to push its borders out to intercept threats to the U.S. before they arrive, it should develop a long range vessel tracking system to give the Coast Guard the ability to know the location of vessels well before they arrive in our territorial waters.

SECURITY GAP: Port Security Programs Are Underfunded.

In July 2003, in accordance with the MTSA, the Coast Guard issued port security regulations for ports, facilities, and vessels. The regulations require port facilities to hire security officers, and install barriers and surveillance systems, all of which were non-existent before 9/11. Unfortunately, the resources provided to our ports have not been sufficient to get the job done. The Coast Guard estimates that ports will spend \$1.1 billion this year and \$5.4 billion over ten years to comply with the regulations.²⁰¹ The only source of funding for security upgrades outside of port authorities' or facility owners' budgets is a port security grant in the DHS Office of Domestic Preparedness. Congress has taken the lead in supporting port security grants by appropriating \$125 million in fiscal year 2004 bringing the total since 9/11 to \$513 million. Despite Congress's support, funding for ports is still \$566 million short of the Coast Guard's first year estimate. Yet, the Administration has only requested \$46 million in its fiscal year 2005 budget for port security grants. In previous budgets, the Administration did not request any funding for port security.

Status of Port Security Grants

USCG 10-Year Estimate	USCG 1-Year Estimate	Appropriated Funds (FY 2002-04)	Admin. FY2005 Request	1 st Year Funding Gap
\$5.4 billion	\$1.125 billion	\$513 million	\$46 million	\$566 million

Ports have completed the assessments to determine what their vulnerabilities are and have developed security measures which will eliminate them. However, the lack of funding forces ports to purchase what they can afford instead what they actually need to increase security.

²⁰¹ *Federal Register* U.S. Coast Guard, Interim Final Rule Facility Security. July 1, 2003. p39319.

SECURITY RECOMMENDATION

Increasing grant funding will ensure ports can pay for adequate security measures which will aid in the prevention of terrorist attacks at America's seaports. While port security efforts require a public-private partnership, federal assistance must increase in order to ensure America's ports are secure without slowing economic activity. Many ports have diverted funding for infrastructure improvements designed to facilitate trade growth, to pay for security. To enable ports to make basic security improvements as quickly as possible, the federal government should fund the \$566 million gap between estimated first year costs and the funds requested in the budget. To provide necessary funding in subsequent years DHS, port authorities, and industry should develop a cost sharing agreement.

Securing Our Borders

The relative ease with which the September 11 hijackers obtained visas and entered the United States revealed glaring weaknesses in our border security systems. While border security has long been a national goal, the September 11 attacks provided renewed urgency to the decades' long task of securing our borders against the entry of terrorists – a monumental challenge due to the geographic dimensions of our borders and the need to maintain the free flow of legitimate travel and commerce. The Administration has properly adopted a “layered” approach to securing our borders, starting with injecting greater security into the visa issuance process abroad and the inspections that take place at American ports-of-entry. While improvements have been made, there has been insufficient investment in programs, infrastructure, and personnel to transform the border into one that both keeps terrorists out of the country and serves the nation’s economic needs in the 21st century. To better protect America from terrorism, while maintaining the economic vitality of the border, the Administration must invest in basic infrastructure at the border, properly staff consulates abroad, the border patrol, and inspection services, and crack down on false identifications. If border security is not a priority, then America will remain vulnerable to those who seek to harm us.

Border security is a tremendous challenge for the U.S. Our borders with Canada and Mexico are more than 7,000 miles long. Substantial portions have inadequate physical security and infrastructure and are not adequately patrolled.²⁰² The security challenge is magnified by the large number of people and goods crossing the border annually. Yearly, over 440 million inspections take place at U.S. air, sea and land ports-of-entry.²⁰³ More than 358 million - over 80% - of these crossings occur at our land borders.²⁰⁴ In 2002, an estimated \$1.4 trillion in imports and \$974 billion in exports passed through our ports-of-entry.²⁰⁵

Members of al Qaeda exploited vulnerabilities in our border security systems to gain entry into the U.S. and carry out the attacks of September 11. All of the 9/11 hijackers received visas from U.S. embassies and consulates.²⁰⁶ At the time that the hijackers applied for visas, none of the names contained in the passports they furnished to State Department consular officers were in State Department databases or the watch list used at the time.²⁰⁷ In total, nineteen 9/11 hijackers entered the U.S. a total of 33 times, and while a few of the terrorists were pulled aside for a more

²⁰²Jeremy Torobin, “C’est La Vie: French Canadians - and God Knows Who Else - Can Easily Slip Into the U.S. on Unguarded Rural Roads,” *CQ Homeland Security*, August 21, 2003.

²⁰³U.S. Department of Homeland Security, *Appendix to the Testimony of Asa Hutchinson, Undersecretary of Border and Transportation Security Before the Select Committee on Homeland Security Subcommittee on Infrastructure and Border Security*, U.S. House of Representatives, January 28, 2004.

²⁰⁴*Ibid.*

²⁰⁵U.S. Department of Homeland Security, *Data Management Improvement Act Task Force - Second Annual Report to Congress*, (Washington, D.C.: December 2003), 1.

²⁰⁶The National Commission on Terrorist Attacks Upon the United States, *Staff Statement No.1 – Entry of the 9/11 Hijackers into the United States*, January 26, 2004.

²⁰⁷*Ibid.*, 4.

intensive inspection, they were subsequently admitted to the U.S.²⁰⁸ The ability of foreign nationals to so easily abuse the visa process and enter our country through legal channels has been the focus of great scrutiny since 9/11. Although new laws have been enacted and the major border agencies have been consolidated into the Department of Homeland Security (DHS), inadequacies remain in key areas that must be addressed if we are to both secure our borders and facilitate the flow of legitimate travel and commerce.

SECURITY GAP: State Department Consular Offices Do Not Have Sufficient Staff to Handle Post-9/11 Policy Changes Directed Toward Securing the Visa Process.

One important aspect of border security is to ensure that individuals who might represent a threat are not permitted to obtain visas. Visa issuance is the responsibility of the State Department's 211 consular offices around the world.

Prior to 9/11, consular offices overseas lacked resources to identify terrorists. Indeed, the National Commission on Terrorist Attacks upon the United States concluded that consular officers at the State Department were not full partners in a national counter-terrorism effort and that consular offices were not provided with sufficient resources to perform this "expanded" mission.²⁰⁹ When visa applications rose by nearly a third between 1998 and 2001, an increase of 2.5 million per year, the number of trained staff did not increase.²¹⁰ This paucity of resources led to increased and often unmanageable work loads for consular officers. For example, in two of the consular offices where the 9/11 hijackers were issued visas, Jeddah and Riyadh, each individual consular officer had "responsibility for processing, on average, about 30,000 applications per year and routinely interviewed about 200 people per day."²¹¹ We know that the five offices that issued visas to the 9/11 terrorists did not have sufficient staff to interview most visa applicants.²¹²

In response to this security gap, the State Department appropriately imposed additional security checks on the visa issuance process and required personal interviews for virtually all visa applicants. Yet, as recently as May, 2003, consular offices were directed to "implement the new interview requirements using existing resources" and directed not to "use overtime to deal with additional workload requirements."²¹³ While the General Accounting Office (GAO) found that consular officers at some posts were able to spend more time reviewing visa applications and interviewing applicants because of the dramatic decrease in visa applications following 9/11, at other posts, the growing demand for visas, coupled with the enhanced security requirements, taxed existing staff.²¹⁴ Although the number of overseas officers in consular affairs increased by 132 officers between fiscal years 2001-03,²¹⁵ the additional staffing has not eliminated extensive delays in the visa process.

²⁰⁸Ibid, 6-7.

²⁰⁹Ibid, 9.

²¹⁰Ibid, 9.

²¹¹Ibid, 9.

²¹²U.S. Department of State, Office of the Inspector General, *Memorandum Report: Review of the Issuance of Visas to the September 11, 2001, Terrorists*, ISP-CA-03-27 (Washington, D.C.: March 2003), 2.

²¹³U.S. Department of State, *Outgoing Telegram, Border Security-Waiver of Personal Appearance for Nonimmigrant Visa Applicants -Revision to the Regulations*, (Washington, D.C.: May 21, 2003).

²¹⁴U.S. General Accounting Office, *Border Security: Visa Process Should Be Strengthened as an Antiterrorism Tool*, GAO-03-132NI, (Washington, D.C.: October 2002), 32-33.

²¹⁵Information provided upon request by the U.S. Department of State.

Furthermore, consular duties continue to expand. Suspension of the two programs that allowed travelers to enter U.S. airports en route to other countries without a visa added to visa applications. The installation of biometric technology at overseas consulates and embassies will require consular officers to fingerprint and photograph visa applicants and check their biographical and biometric information against multiple government databases. Additionally, according to the State Department, citizens of many of the 27 countries whose nationals currently are not required to obtain visas to travel to the U.S. ("visa waiver countries") may be required to apply for visas because they will not meet the statutory deadline²¹⁶ for embedding biometric identifiers in their passports.²¹⁷ This eventuality may result in a doubling of visa applications by "upwards of five million additional visas."²¹⁸

While the State Department Diplomatic Readiness Initiative plan proposes to hire over 1100 new civil and foreign service officers by 2005, a systematic assessment of consular staffing and administrative support needs must be undertaken when additional responsibilities are assigned to consular officers. The addition of 93 new consular positions in fiscal year 2004 and 60 new requested positions for fiscal year 2005²¹⁹ is encouraging. If the number of visas increases to pre-9/11 levels, however, there remains real concern about the ability of our consulates to process foreign travelers.

SECURITY RECOMMENDATION

To secure the visa process and facilitate legitimate travel and commerce, the Administration must extend our borders to our embassies overseas. Critical in this expansion is an investment in our consular officers, our first line of defense against those who may seek to harm America. To achieve optimal homeland security while preventing backlogs in the visa issuance process, the Administration should assess the adequacy of staffing and infrastructure for consular operations to ensure that officers have sufficient time to review all applications, conduct interviews, and check all relevant databases before authorizing individuals to enter the U.S.

SECURITY GAP: Truck Cargo is Not Comprehensively Screened for Weapons of Mass Destruction.

As explained in the previous chapter on *Securing Our Ports*, radiation portal monitors are detection devices through which cargo trucks can be driven to screen for nuclear or radiological material. These portals can be integrated into normal operations at border crossings so they do not slow the flow of commerce.

In light of the significant threat that a nuclear or radiological weapon could be smuggled into the U.S. in a cargo truck, radiation portals have not been installed quickly enough at our land borders. Instead, inspectors at many border crossings use equipment incapable of detecting a nuclear or radiological weapon, such as personal radiation pagers.

²¹⁶Enhanced Border Security and Visa Entry Reform Act of 2002, (P.L. 107-173).

²¹⁷U.S. Department of State, *Testimony of Maura Harty, Assistant Secretary, Bureau of Consular Affairs Before the Select Committee on Homeland Security Subcommittee on Infrastructure and Border Security, U.S. House of Representatives*, January 28, 2004.

²¹⁸Ibid.

²¹⁹Ibid.

The Bureau of Customs and Border Protection (CBP) has a plan to deploy radiation portal monitors at major border crossings. So far, portals have been installed at 50 percent of the northern border ports of entry. Funds have been appropriated to complete installation on the northern border, but the project will not be completed until later this year. The fiscal year 2005 budget requests \$50 million for radiation portal installation, but this level of funding would only complete between 25 to 50 percent of the southern border crossings. Thus, by the fourth anniversary of the September 11 attacks, the southern border still will not have a comprehensive detection system installed to screen cargo for weapons of mass destruction.

SECURITY RECOMMENDATION

DHS should move faster to install radiation portal monitors at all border crossings and not rely on personal radiation detectors.

SECURITY GAP: Pre-Clearance and Pre-Inspection Programs Have Not Yet Been Widely Implemented to Enable Inspectors to Focus on High-Risk Traffic.

One of the keys to enhancing border security is to expedite the flow of low-risk individuals through the system so that inspectors can provide greater scrutiny to those more likely to be security risks. Clogged borders with large traffic backups put pressure on inspectors to cut corners. Programs that “pre-clear” individuals to cross the border help reduce congestion and therefore enhance security. Likewise, “pre-inspection” programs reduce backlogs and enhance security at our borders by processing individuals through customs and immigration requirements before they board international flights to come to the United States. Other travelers inspected at our borders, therefore, can be given greater scrutiny.

- **Land Border Pre-Clearance Programs – Individuals**

The Administration should place greater emphasis on infrastructure in its implementation of its northern border pre-clearance program – NEXUS – and its southern border counterpart – Secure Electronic Network for Travelers Rapid Inspection (SENTRI). These programs subject enrollees to intensive background checks which, if successful, allow them to cross the border through dedicated lanes and receive an expedited inspection. NEXUS is operational at 10 of the 120 northern border crossings,²²⁰ while SENTRI is present at only three of the 43 southern border crossings. The benefits of these programs are substantial. The majority of NEXUS/SENTRI inspections generally take approximately 11 seconds or less compared to one minute for travelers using regular lanes,²²¹ while still providing a more thorough background review of the traveler.

Neither program is as effective as it could be because pre-cleared passengers are often unable to get to the dedicated inspection lanes due to traffic backups. Improvements, such as building unimpeded access lanes for pre-cleared travelers and equipping additional inspection lanes with

²²⁰Information was provided by the U.S. Department of Homeland Security upon request. The U.S./Alaska border with Canada is not included.

²²¹U.S. General Accounting Office, *Land Border Ports of Entry: Vulnerabilities and Inefficiencies in the Inspections Process*, GAO-03-782, (Washington, D.C.: July 2003), 36.

pre-clearance technology, are necessary.²²² Expansion of enrollment sites for both programs, to allow travelers to enroll in the program closer to where they live or work, or when they apply for visas at the embassies, would also help to reduce congestion and improve security at the border.

SECURITY RECOMMENDATION

The Administration should expand pre-clearance programs to all major ports-of-entry along the northern and southern border and create dual-use lanes equipped with NEXUS and SENTRI technology to allow inspectors at the border additional flexibility in the inspections process. Access lanes should be expanded to facilitate the free flow of traffic and rapid inspection of those who have been pre-cleared. Additionally, to achieve maximum utility of the pre-clearance process, the Administration should consider creating pre-clearance programs for those crossing our borders on foot or using mass transit. Enrollment of travelers in the SENTRI program should be initiated in the visa application process at embassies and consulates in Mexico or at least made available at such locations. Finally, to deliver border security, pre-clearance technology must actually work. The Administration should ensure that sufficient funds are dedicated for regular upgrade and maintenance of NEXUS and SENTRI systems.

- **Land Border Pre-Clearance Programs – Cargo**

An estimated 13 million cargo containers and commercial trucks enter the U.S. every year. Screening these containers without bringing commercial traffic to a grinding halt is an immense challenge. After 9/11, the Administration launched the Free and Secure Trade (FAST) program. Under the FAST program, importers, commercial carriers and truck drivers qualify for expedited clearance at the border if they submit fingerprints, pass a criminal background check, submit to an interview, and drive for companies enrolled in the Customs-Trade Partnership Against Terrorism (C-TPAT). Like NEXUS and SENTRI, the FAST program enables low-risk traffic to proceed through inspections quickly while allowing inspectors to direct greater attention to higher-risk cargo trucks.

The first FAST/NEXUS lane opened in Port Huron, Michigan, on January 9, 2004, and there are FAST lanes at eight major crossings along the northern border. While FAST is a good approach to ensuring cargo can move efficiently across the border without jeopardizing security, the Administration has failed to address security lapses in this program. As set forth in the previous chapter on *Securing Our Ports*, only 141 of the 5,300 C-TPAT members have had their security measures validated by DHS, leaving many FAST members who received the benefit of reduced inspections at the border but have not demonstrated that they have improved their security.

In October 2003, DHS launched a pilot FAST program for Mexican trucks crossing the southern border in El Paso. FAST Mexico is different than the program on the northern border in that it requires additional security measures, the most noteworthy of which is that cargo containers must have a tamper-resistant seal.

There are no funds in the fiscal year 2005 budget for expanding the FAST program on either the northern or southern border or for FAST infrastructure improvements.

²³U.S. Department of Homeland Security, *Data Management Improvement Act (DMIA) Task Force - Second Annual Report to Congress*, (Washington, D.C.: December 2003), 112.

SECURITY RECOMMENDATION

For FAST to be a credible security program, CBP should accelerate the security validations of FAST/C-TPAT members. Furthermore, the Administration should expand the FAST program to cover all major ports on entry on both the northern and southern border and increase FAST access lanes to speed inspections. Finally, FAST trucks crossing the northern border should also be required to use tamper-resistant seals.

- **Airport Pre-Inspection Programs**

The Administration is not sufficiently expanding pre-inspection programs at foreign airports. Pre-inspections subject travelers to the full U.S. inspections process at a foreign airport where a person's travel originates. This type of pre-screening reduces backlogs at our ports of entry and could prevent dangerous individuals from getting on a plane in the first place.

To date, pre-inspection programs are in airports at only five countries- Canada, Ireland, Bermuda, the Bahamas and Aruba. Yet, in fiscal year 2003, 13.5 million people, or 49% of all overseas visitors, entered the United States from "visa waiver" countries.²²³ These individuals receive little scrutiny before boarding an airplane to the U.S. Placing pre-inspection programs in the airports of visa waiver countries would require that citizens of visa waiver countries receive a customs and immigration check prior to their arrival in the U.S.

SECURITY RECOMMENDATION

The Administration should institute pre-inspection programs in visa waiver countries and other nations with large numbers of travelers to the U.S.

SECURITY GAP: Insufficient Infrastructure Investments Have Been Made to Allow Border Security Programs – Including US-VISIT – To Be Implemented Without Harming the Economies of Border Communities.

A substantial investment in border infrastructure is needed in order to provide security without inhibiting trade. This is especially true at our land ports of entry. For example, layouts of inspection plazas, space limitations, limited number of inspection booths and lanes all affect the flow of traffic.²²⁴ These infrastructure problems pose a unique challenge to border security because land borders handle large volumes of travelers, receive little and usually no advance information about people or cargo, and involve both commercial freight and passenger inspections. Indeed, the stress placed on our borders by the pressure of commerce is dramatic. A small delay in the inspections area can lead to a delay of several hours in getting into the U.S.

²²³U.S. Library of Congress, Congressional Research Service, "Visa Waiver Program," RL 32221, (Washington, D.C.: February 10, 2004), i.

²²⁴U.S. Department of Homeland Security, *Data Management Improvement Act Task Force - Second Annual Report to Congress*, (Washington, D.C.: December 2003), 34.

For example, the peak wait time at the Blaine Peace Arch in Washington state could increase by more than eleven hours if the average inspection increases by only nine seconds.²²⁵ Backups and delays place pressure on security programs; if travelers and businesses cannot get through the border in a timely fashion, pressure will build to reduce, modify, or eliminate security measures.²²⁶ Not only do delays impact security, but backups at the land borders cause traffic congestion and environmental pollution in border communities.²²⁷ It is vital to our homeland and economic security that border security programs facilitate and expedite the inspections process, not result in long delays and confusion at the border.

Enhancing security without hindering commerce requires investments in basic infrastructure and technology to limit the amount of time inspections take. Many land ports of entry today have inadequate infrastructure. A total of 64 ports have less than 25 percent of the required space in the inspections area.²²⁸ Approach highways and border inspection facilities were considered inadequate and overburdened even before 9/11.²²⁹ According to the Data Management Improvement Act Task Force, “resources to expand and improve the infrastructure to support growth in work load and staffing have not kept pace, creating infrastructure weaknesses.”²³⁰

The need for additional infrastructure investments is critical given the planned implementation of the United States Visitor Immigrant Status Indicator Technology (US-VISIT) program at land borders. The US-VISIT program is the system being put in place at our airports, seaports, and land borders to comply with the statutory mandate to develop an automated system to track the arrival and departure of certain foreign visitors to the U.S. The system is designed to add integrity to our immigration process by capturing the biometric information of certain foreign visitors when they apply for a visa at U.S. embassies and consulates or arrive at U.S. ports of entry. On arrival, visitors will have their fingerprints and photographs taken, which will then be compared to data in the US-VISIT database to ensure that the person who is trying to enter the country is the same person who received the visa abroad. Personal and biometric information is also compared against certain government immigration and criminal databases to determine whether the visitor should be permitted to enter the U.S. Additional database review also occurs post-admission to the U.S. Finally, when the system is fully completed, visitors will record their departure from the U.S., which will enable authorities to identify visitors that have overstayed their visas.

The US-VISIT program began operations at 115 airports and 14 seaports on January 5, 2004. The gradual and limited nature of the program’s initial stages enabled operations to proceed relatively smoothly, but allowed security gaps to remain. For example, citizens of the 27 mostly-European and English speaking “visa waiver” countries are currently exempt from the program. Thus, under current procedures, people like British national Richard Reid, the “shoe bomber,” or French national Zacarias Moussaoui, the alleged al Qaeda operative, would not be subject to an US-VISIT inspection. As Assistant Secretary of Homeland Security C. Stewart Verdery, Jr.

²²⁵U.S. General Accounting Office, *Department of Homeland Security’s US-VISIT Program*, Staff Briefing, (Washington, D.C.: October 23, 2003), 22.

²²⁶Prior to the implementation of the US-VISIT program, a memo was circulated to Directors of Field Operations, instructing them that if wait times at inspections stations approached one hour, mitigation strategies should be implemented that would reduce the number people being enrolled in US-VISIT.

²²⁷U.S. Department of Homeland Security, *Data Management Improvement Act Task Force, Second Annual Report to Congress*, (Washington, D.C.: December 2003), 35.

²²⁸*Ibid*, 33.

²²⁹*Ibid*, 33.

²³⁰*Ibid*, 33.

noted, "It is a problem with the VISIT system that visa waiver travelers are not enrolled."²³¹ Moreover, the challenges of implementing US-VISIT at the land borders are far greater than what has been achieved thus far since, of the over 440 million inspections that take place per year, only 20 percent occur at air and sea ports while 80 percent are at our land borders.²³²

Expanding US-VISIT to close the security gaps currently in the system and to cover the land borders will require investment in infrastructure.²³³ Depending on how the Administration chooses to implement the US-VISIT program at land ports-of-entry, most land ports will at the very least require additional space in already overburdened inspection facilities in which to place US-VISIT equipment. Additional space will also be needed to accommodate visa holders while they await enrollment. Implementing the "exit" requirements of US-VISIT, especially at land borders, would be a substantial undertaking. Not only would exit-kiosks have to be installed at all airports and seaports, but depending on Administration implementation plans, an entirely new exit infrastructure may have to be built (where none currently exists) at all land border crossings.

Land border communities are deeply concerned that US-VISIT requirements will be implemented without the needed infrastructure investments, which will lead to large delays upon entry to and departure from the U.S., increased traffic congestion and pollution on both sides of the border, and a reduction in the economic vitality of the border region.²³⁴ The Administration has done an inadequate job reaching out to these communities to learn their concerns about the possible impact of US-VISIT implementation and engaging them in the planning process.

SECURITY RECOMMENDATION

The Administration has an historic opportunity to strengthen our borders and border communities by investing in roads and inspection facilities that will allow for secure inspections while facilitating legitimate travel and commerce. In order to create an economically vibrant and secure border, the Administration should expand or restructure inspections areas; identify technology to provide a secure and expedited inspections process; and expand highways and access roads.

The Administration should also provide for a full evaluation of the impact of US-VISIT on border communities and commerce. Finally, the Administration should initiate an immediate outreach program to border communities to discuss US-VISIT implementation and provide community leaders the opportunity to fully participate in the planning and implementation process.

²³¹Jeremy Torobin, "U.S. Proposes Stationing Passenger Screeners in Foreign Airports," *CQ Homeland Security*, February 18, 2004.

²³²U.S. Department of Homeland Security, *Data Management Improvement Act Task Force - Second Annual Report to Congress*, (Washington, D.C.: December 2003), 15.

²³³U.S. Department of Homeland Security, *Data Management Improvement Act Task Force - First Annual Report to Congress*, (Washington, D.C.: December 2002), 33.

²³⁴U.S. Department of Homeland Security, *Data Management Improvement Act Task Force - Second Annual Report to Congress*, (Washington, D.C.: December 2003), 34-35.

SECURITY GAP: Border Security Programs Lack Access to a Reliable, Comprehensive and Integrated Terrorist Watch List.

As set forth in the previous chapter on *Preventing Attacks By Improving Intelligence*, two and a half years after the events of 9/11, the Administration is still struggling to address a key problem in securing the U.S. – information sharing. The ability of border security programs like US-VISIT, NEXUS and SENTRI to help secure America depends largely on the Administration's ability to enhance the intelligence capacity of these systems and improve the interconnectivity, reliability, and accuracy of its databases. Specifically, border security must have a "real-time" link to a comprehensive, constantly-updated terrorist watch list. Such a watch list does not currently exist, and current estimates are that integration of existing watch lists will not be completed until mid-summer 2004. That estimate, however, does not contemplate the secure, real-time linkage of the terrorist watch list with border programs and personnel conducting border inspections. There is no official Administration estimate of the time needed to fully link these programs with all government terrorist-related information.

As the report issued by Democratic Members of the Select Committee on Homeland Security, *Keeping Terrorists Out of America By Unifying Terrorists Watch Lists*, explains, one key aspect of a functional terrorist watch list is to have a mechanism for correcting inaccuracies and removing names that should not be on the list.²³⁵ This is especially true for border operations, because such inaccuracies will result in repeated and prolonged inspections of travelers who pose no threat but serve to distract law enforcement personnel from more pressing inspections.

SECURITY RECOMMENDATION

The Administration should move rapidly to ensure that border security programs are linked to a comprehensive, integrated terrorist watch list and that border personnel have real-time access to the most up-to-date terrorist watch list information available. The Administration should create a venue through which inaccuracies in databases, systems and watch lists that inaccurately and repeatedly flag travelers who are not threats to the U.S. are addressed.

SECURITY GAP: There is No Post-9/11 Comprehensive Border Staffing Strategy.

Just as sufficient infrastructure is necessary to achieve both security and the free flow of commerce at the border, it is also necessary for the government to have the appropriate number of inspectors and border patrols in order to achieve its border security goals. Yet, more than two years after the 9/11 attacks, the Administration still has not proposed a comprehensive staffing strategy to secure our borders.

When inspectors from the U.S. Customs Service and Immigration and Naturalization Service (INS), and agents from the Border Patrol, were integrated into the CBP in 2003, each agency had a strategic staffing model that had been in place prior to the 9/11 attacks. These models reflected the agencies' missions at the time, which largely included stemming the flow of drugs and illegal

²³⁵ Democratic Members of the House Select Committee on Homeland Security, *Keeping Terrorists Out of America by Unifying Terrorist Watch Lists*, November 2003.

immigrants into the country across the U.S.-Mexico border. Indeed, the pre- 9/11 Border Patrol strategies are still displayed on the CBP website as “current” strategies. However, these staffing strategies do not reflect security concerns raised after the 9/11 attacks, such as longer operating hours at certain ports-of-entry, heightened security needs when the country moves to a higher alert level, such as "Code Orange," and new technology (such as camera arrays) that is available to monitor the unstaffed border areas.

The Administration has taken some steps to increase northern border security, but this has occurred at the expense of security on our southern border. For instance, the number of Border Patrol agents on the northern border was increased from 334 (in 2001) to 1,006²³⁶ last year only by reassigning hundreds of Border Patrol agents from the southern border. The Administration increased Border Patrol staffing to comply with the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) and the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act).²³⁷ While these two bills did not address staffing issues on the southern border, the USA PATRIOT Act did require the Administration to triple the number of Border Patrol agents, border crossing inspectors and support staff over 2001 levels on the northern border. Similarly, the Border Security Act required the Administration to add 200 border crossing inspectors each year over USA PATRIOT ACT levels. Only one of the many targets – Border Patrol staffing – has been met.

USA PATRIOT ACT OF 2001¹				
<i>Northern Border Customs & Border Protection Component</i>	<i>Staffing levels as of October 2001</i>	<i>Staffing level required</i>	<i>Staffing Level (as of 10-03)</i>	<i>What is still needed</i>
Border Patrol agents	348²	1,044	1,006³	38
Customs Inspectors	1,059²	3,177	1,589³	1,588
Immigration Inspectors	524²	1,572	1,132³	440
ENHANCED BORDER SECURITY ACT⁴				
Required immigration inspector levels – Fiscal Year 2003	(base is triple October, 2001 levels) 1,572	1,772	1,132	640
Fiscal Year 2004		1,972	1,132	840
Fiscal Year 2005		2,172	1,132	1,040
Fiscal Year 2006		2,372	1,132	1,240

²³⁶ Figures provided by the U.S. Department of Homeland Security, October 4, 2003.

²³⁷ USA PATRIOT Act (P.L. 107-56); Border Security Act (P.L. 107-173).

Sources: (1) USA PATRIOT Act; (2) House Committee on Government Reform Report, "Federal Law Enforcement At The Borders And Ports Of Entry: Challenges & Solutions," July 2002; (3) Letter from Department of Homeland Security to Congressman Jim Turner (December 11, 2003); (4) Border Security Act.

A comprehensive border staffing strategy is essential because it is the "master plan" directing where to place personnel, technology, and infrastructure, and in what order these needs should be addressed. The cornerstone of any comprehensive plan is the well-trained and experienced personnel assigned to guard our borders – and we must know where to most effectively place them.²³⁸

SECURITY RECOMMENDATION

The Administration should immediately develop and implement a comprehensive national border staffing strategy that will allow DHS to effectively deploy its personnel (border crossing inspectors, Border Patrol agents, and support staff) and technology. The staffing strategy should maintain the border agencies' original missions of preventing drug traffic and illegal immigrants from entering the U.S.; meet staffing levels established in the USA PATRIOT Act and Border Security Act; and build in flexibility to meet changing security needs of the future. The Administration should work with Congress to amend all relevant laws, if necessary, and work with Congress to ensure that updated staffing models are completed and fully implemented.

SECURITY GAP: Unauthorized Persons Can Enter the United States Using Fraudulent Driver's Licenses and Other Forms of Identification.

Counterfeit or fraudulent identification (ID) cards are a serious threat to our homeland security because they provide terrorists with the ability to enter the United States and easily move about society - without being detected. Counterfeit ID cards are readily available today because they are hard to detect among the numerous legitimate versions of driver's licenses and state-issued ID cards. For example, there are currently 240 legitimate versions of state driver's licenses and IDs and more than 50,000 versions of legitimate birth certificates.²³⁹ These documents have proliferated because there are no uniform standards for the appearance of ID cards – and the states and territories have not coordinated their activities in this area.

Counterfeit IDs are also easily produced with off-the-shelf technology.²⁴⁰ This is evidenced by the government's continuing work to break up large counterfeit ID rings, such as DHS' Bureau of Immigration and Customs Enforcement "Operation Card Shark," which broke up a large counterfeit ID ring in the Adams Morgan section of Washington, D.C. in 2003.²⁴¹

²³⁸U.S. Library of Congress, Congressional Research Service, *Terrorism: Automated Lookout Systems and Border Security Options and Issues*, RL31019, William J. Krouse and Raphael F. Perl, June 18, 2001, 9.

²³⁹U.S. Department of Homeland Security, *Testimony of Asa Hutchinson, Under Secretary for the Border and Transportation Directorate Before the Committee on Finance, U.S. Senate*, September 9, 2003.

²⁴⁰U.S. General Accounting Office, *Security: Counterfeit Identification and Identification Fraud Raise Security Concerns*, GAO-03-1147T, (Washington, D.C.: September 9, 2003), 6.

²⁴¹Mary Beth Sheridan, "Norton Calls ID Markets Terror Magnet," *Washington Post*, August 6, 2003, sec. B.

Counterfeit IDs are a particular threat to our borders because border crossing inspectors may accept ID documents (state driver's licenses, birth certificates, or other form of identification) as proof of citizenship from Americans re-entering the U.S.²⁴² Assistant Secretary of Homeland Security, C. Stewart Verdery, Jr., described the current policy of accepting ID cards as "a giant loophole in our improving exit-entry system."²⁴³ In fact, GAO demonstrated the ease with which it is possible to enter the U.S. by posing as an American citizen and displaying fraudulent IDs.²⁴⁴ In its investigation, GAO produced counterfeit documents which were used to obtain a valid driver's license from another state, enter the U.S. from various Western Hemisphere countries, and access sensitive areas in airports.²⁴⁵

Counterfeit ID cards also enable terrorists to move freely about the country because these ID cards are increasingly considered as unquestionable proof of identity by many government agencies and private sector businesses. For example, counterfeit ID cards can be used to gain access to government buildings, obtain Social Security numbers for fictitious identities, and purchase firearms. These documents are also the basis for the distribution of important U.S. identity documents, such as passports and Social Security cards.²⁴⁶

Today, there is no coordinated federal approach in addressing this issue, despite previous efforts to do so.²⁴⁷ However, the need to increase border security following the 9/11 attacks, and the failure of states to promote national security by adopting uniform standards for ID documents, provides a justification for the federal government to take the lead in establishing national standards for state ID cards and driver's licenses. The American Association of Motor Vehicle Administration (AAMVA) has developed and vetted a set of uniform standards and procedures that could serve as a starting point for establishing these standards.

SECURITY RECOMMENDATION

The Administration should establish a uniform set of standards for all state driver's licenses and official state identification cards. Setting these standards would help reduce the likelihood of unauthorized persons entering the United States by using fraudulent documents.

²⁴² U.S. General Accounting Office, *Security: Counterfeit Identification and Identification Fraud Raise Security Concerns*, GAO-03-1147T (Washington, D.C.: September 9, 2003), 3.

²⁴³ Jeremy Torobin, "U.S. Proposes Stationing Passenger Screeners in Foreign Airports," *CQ Homeland Daily*, February 18, 2004.

²⁴⁴ U.S. General Accounting Office, *Security: Counterfeit Identification and Identification Fraud Raise Security Concerns*, GAO-03-1147T (Washington, D.C.: September 9, 2003), 1.

²⁴⁵ Ibid.

²⁴⁶ Shane Ham & Robert D. Atkinson, "Modernizing the State Identification System: An Action Agenda," *Progressive Policy Institute*, February 2002, 1.

²⁴⁷ Sec. 656(b) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA) (Division C of P.L. 104-208) established uniform standards for state driver's licenses; however, its implementation was blocked by a provision of the Fiscal Year 1999 Department of Transportation appropriations bill (P.L. 105-277), which prohibited the expenditure of any funding under that act for the purposes of implementing regulations related to Section 656(b) of IIRIRA.

SECURITY GAP: The Administration Has Failed to Effectively Coordinate Its Mission to Secure the Northern and Southern Border.

The northern and southern borders are unique because of the strong economic, political and cultural ties between the US, Canada and Mexico. More than 100 million people cross the U.S.-Canada border annually, and 90 percent of the Canadian population live within 100 miles of the US-Canada border.²⁴⁸ Over 300 million people cross the U.S.-Mexico border each year and an estimated 10 million live in the U.S.-Mexico border region.²⁴⁹ Therefore, bilateral cooperation is critical to ensure enhanced border security. Additionally, it is important that security along our borders be overseen in a coordinated manner among federal, state and local law enforcement and first responders. Currently, no single government official is responsible for coordinating law enforcement, immigration, and homeland security programs for the entirety of a border region. While bilateral “Smart Border” agreements have been reached with both Canada and Mexico to improve border functions, ensure security, and promote travel and trade,²⁵⁰ concern exists that the implementation of these agreements is losing momentum.²⁵¹

SECURITY RECOMMENDATION

To better coordinate governmental functions along the border, the Administration should create Northern Border and Southern Border Coordinators in the Department of Homeland Security reporting directly to the Undersecretary for Border and Transportation Security. These coordinators will help further implement the “Smart Border” agreements with Canada and Mexico and provide enhanced communication among federal agencies with border responsibilities and between federal, state and local officials from border communities.

²⁴⁸Deborah Waller Meyers, “Does Smarter Lead to Safer,” *Migration Policy Institute Insight*, June 2003, 2.

²⁴⁹Ibid.

²⁵⁰The U.S., Canadian and Mexican governments signed two smart border agreements. The U.S. and Canada signed the Smart Border Declaration on December 12, 2001 and the U.S. and Mexico signed the Border Partnership Agreement on March 22, 2002.

²⁵¹Andre Belelieu, “The Smart Border Process at Two: Losing Momentum?” *Hemisphere Focus*, Center for Strategic and International Studies, December 10, 2003.

Securing Our Skies

Terrorist attacks involving aircraft continue to be of great interest to al Qaeda and a major threat to the security of the United States. Despite massive federal investments in aviation security since September 11, major security gaps remain. Serious deficiencies have been revealed in many of the “layers” of security the Transportation Security Administration has put in place at our nation’s airports. To close security gaps in the aviation system, the Transportation Security Administration should improve the performance of its screening workforce, take aggressive steps to secure air cargo, adopt new measures to defend aircraft against missile attack, and improve controls over access to sensitive airport locations and airplanes.

The terrorist attacks of September 11 exploited several shortcomings in U.S. aviation security. The hijackers were not stopped from boarding aircraft by pre-screening systems or security inspections and were able to gain control of aircraft once airborne. The response to these heinous attacks was, in part, to create a new federal agency to ensure the security of passenger and cargo aircraft. Under demanding statutory deadlines, the Transportation Security Administration (TSA) hired an army of security screeners, reaching a one-time high of 54,600 personnel. Congress has provided TSA with a total of \$10.7 billion for passenger and baggage screening.²⁵²

The threat of terrorist attacks on aircraft, or using aircraft as weapons, remains vivid. When raising the nation’s threat level to “High” on December 21, 2003, Secretary Ridge stated that, “Recent reporting reiterates ... that al-Qaida continues to consider using aircraft as a weapon. And they are constantly evaluating procedures both in the United States and elsewhere to find gaps in our security posture that could be exploited.”²⁵³

Congressional mandates and TSA regulations have led to a number of additional steps over the past two years to improve aviation security. The number of air marshals riding on flights has increased from 33 on September 11 to thousands.²⁵⁴ All U.S. passenger aircraft, as well as foreign flights arriving or departing in the United States, now have hardened cockpit doors. In its first year and a half of airport screening, more than 7.5 million prohibited items, including nearly 2.3 million knives, 1,437 firearms and 49,331 box cutters were taken from passengers.²⁵⁵ Recently, several commercial flights were delayed, cancelled, or escorted by military aircraft when deemed to be at significant risk of a terrorist attack. Finally, TSA has rightly emphasized a

²⁵² Appropriation levels from Public Laws 107-87, 107-117, 108-7, 108-11, 108-90, and 108-206. The figure includes fees levied on passenger tickets.

²⁵³ See U.S. Department of Homeland Security Press Office, “Threat Level Raised, Remarks by Secretary of Homeland Security Tom Ridge,” December 21, 2003.

<http://www.whitehouse.gov/news/releases/2003/12/20031221.html>.

²⁵⁴ The exact number of federal air marshals (FAMs) is classified, but is in the few thousands. On November 25, 2003, the FAM program was moved from TSA to the DHS Bureau of Immigration and Customs Enforcement.

²⁵⁵ Transportation Security Administration, “State of Aviation Security Fact Sheet,” September 29, 2003. <http://www.tsa.gov/public/display?theme=8&content=0900051980057f92>.

“layers of defense” strategy, employing multiple protective measures to guard against terrorist attack.

However, despite the progress and the vastly heightened public awareness to the threat of hijacking, major vulnerabilities remain in our aviation system. Several of the layers of defense have significant security gaps. The TSA must address ongoing problems with aviation security, including concerns about the efficacy of airport screening, the lack of security for air cargo, the potential threat from shoulder-fired missiles, and unauthorized access to aircraft or other secure airport areas.

SECURITY GAP: Passenger and Baggage Screening Allows Significant Numbers of Dangerous Items Aboard Aircraft.

The DHS Office of the Inspector General, the General Accounting Office (GAO), and the TSA’s own investigation team have all conducted undercover investigations and found that prohibited items – including, according to media reports, firearms and simulated explosive devices – are still passing through TSA screening checkpoints. Comparisons with similar investigations conducted before TSA started its screening operations show that much improvement is still needed.²⁵⁶ Security tests by media groups and private citizens have also demonstrated flaws in the security screening process.²⁵⁷ Statements by TSA employees suggest that a number of checked bags are not even subjected to screening measures, in one case alleging that “federal baggage screeners run only a small portion of suitcases through explosives-detection devices.”²⁵⁸ Current screening systems are not capable of routinely catching passengers that have hidden explosives on themselves.

Appropriate screener staffing levels, better detection technology, and a stronger training program would greatly decrease these security shortfalls.

- **Screener Staffing**

Having the appropriate number of screeners at airport security checkpoints is critical to aviation security. Too few screeners leads to increased passenger wait times, which in turn applies pressure on TSA personnel to take security shortcuts. According to a recent GAO study, insufficient screener staffing has led to an inability to fully utilize detection equipment and to access all training programs.²⁵⁹ These problems stem from an October, 2003 congressional decision to cap the TSA screener level at 45,000 due to concerns about escalating costs and a

²⁵⁶ Specific results of screener testing are sensitive and not publicly released. Information obtained from General Accounting Office and Department of Homeland Security Office of Inspector General. Previous FAA studies uncovered a 20 percent failure rate to identify prohibited items, and failure rates increased when tests were made to more accurately predict how terrorists might try to conceal weapons (GAO, *Vulnerabilities in, and Alternatives for, Preboard Screening Security Operations*, GAO-01-1171T, (Washington: U.S. General Accounting Office, September 25, 2001), 5-6.

²⁵⁷ In one investigation since 9/11, it was reported that prohibited items cleared passenger security for all 14 flights attempted at 11 airports. Maki Becker and Greg Gittrich, “Weapons Still Fly at Airports: News Boards 14 Jets with Contraband Despite Security Push,” *Daily News*, September 4, 2002, 7.

²⁵⁸ Confidential interviews between TSA employees and staff of the House Select Committee on Homeland Security. See also Sharon Linstedt, “Ex-Chief Calls Gaps in Security ‘Serious’,” *The Buffalo News*, February 11, 2004, B1.

²⁵⁹ GAO, *Airport Security: Challenges to Airport Passenger and Baggage Screening*, GAO-04-440T, (Washington: U.S. General Accounting Office, February 12, 2004), 3, 16.

growing screener workforce.²⁶⁰ However, no comprehensive personnel study has been conducted to ensure that this personnel level is the number necessary to adequately screen all passengers and checked baggage. Nonetheless, TSA has sought to comply with this congressional mandate and has reset staffing levels at all airports. As of February 9, 2004, TSA screener staffing was below the overall national cap of 45,000.²⁶¹

SECURITY RECOMMENDATION

The TSA, working with airport authorities, should conduct a comprehensive study to determine how many screeners are actually necessary to implement appropriate security procedures at all checkpoints. This study should include analysis of current passenger traffic, which varies regularly with flight schedules and seasonal demand, in order to provide the number of screeners required for full security. The TSA should recognize in this study that the presence of long passenger delays at security checkpoints is likely to place pressure on screeners to take shortcuts in security, and account for such a possibility accordingly. Congress should then revise the 45,000 screener cap imposed in 2003, if warranted, and it should provide TSA with the funding required to support a screener workforce that meets those demands.

• Screening Technology

The technology for both passenger and baggage screening deployed at U.S. airports is still substantially the same as what was in place before September 11²⁶² and TSA has not acted aggressively to develop and deploy new technology. In fact, in fiscal year 2003, TSA shifted \$60 million out of \$75 million appropriated for technology development to cover shortfalls in its current operating budget.

TSA and private companies have identified promising technologies that can better locate and identify concealed explosives and other dangerous items, which would greatly improve screeners' ability to prevent these items from getting onto aircraft. For example, technologies exist that can detect explosives residue on passengers, which cannot be identified with currently deployed detectors. This particular security gap was exposed when would-be terrorist Richard Reid was able to bring roughly ten ounces of explosives onto an American Airlines international flight, and he was only stopped from carrying out a terrorist attack by alert passengers. According to GAO, "TSA is funding [research and development] on several technologies designed to improve the screening of checked baggage and passengers at the nation's airports. However, while the majority of these technologies are scheduled for pilot testing within the next 12 to 18 months, they are not scheduled to be deployed in quantity for 2 to 5 years."²⁶³

²⁶⁰ House Report 108-280 accompanying "Department of Homeland Security Appropriations Act of Fiscal Year 2004." (P.L. 108-90).

²⁶¹ Briefing from DHS Budget Office staff for Select Committee on Homeland Security staff, February 9, 2004.

²⁶² See testimony of Stephen McHale, Deputy Administrator, Transportation Security Administration. U.S. House, Committee on Government Reform, *Knives, Box Cutters, and Bleach: a Review of Passenger Screener Training, Testing, and Supervision* Hearing, November 20, 2003. According to McHale, "I agree with you completely that the technology we're using is somewhat better than 9/11 but not a lot. It is the same type of technology."

²⁶³ GAO, *Airport Security: Challenges to Airport Passenger and Baggage Screening*, GAO-04-440T, (Washington: U.S. General Accounting Office, February 12, 2004), 32.

Additionally, TSA has not adequately deployed technology that already exists. It has failed to install explosives detection technology needed to fully screen checked baggage at a number of airports, despite a legal requirement to do so this by December 31, 2003.²⁶⁴ At least five airports are still reportedly using hand inspections, canine teams, and passenger-bag matching to secure baggage placed on commercial aircraft.²⁶⁵ One reason that screening equipment has not been installed at all airports is that current detectors are too large to fit into many existing airport structures.²⁶⁶ New technologies can provide smaller, but equally or more capable, screening equipment that would fit into existing infrastructure.

Another technology, the Threat Image Projection (TIP) System, is not being fully deployed at U.S. airports. The system tests screener performance by rating their ability to identify weapons that virtually are inserted by the detection equipment software into images of bags going through the screening process. The TIP system had been discontinued at passenger screening checkpoints after September 11²⁶⁷ but has recently been restored. However, the system is not used in screening of checked baggage.²⁶⁸

SECURITY RECOMMENDATION

The TSA should invest more in developing, evaluating, and deploying screening technologies. Better technology will improve current screening performance and provide an ability to identify objects that are currently undetectable so as to decrease the likelihood of an armed hijacking or explosion aboard a passenger airplane, and minimize disruption at airports. TSA should increase the use of pilot programs and other means to rapidly deploy new technologies into airports.

- **Screener Training**

During the TSA's two years of operation, a number of problems relating to screener training have been revealed. The TSA addressed most of these issues once they were publicized, but it has not demonstrated a proactive approach to ensuring proper training among the screener or supervisory workforce.

All TSA screeners are required to undergo roughly 100 hours of training, consisting of classroom learning, written tests, and on-the-job skills training. Screeners are also subject to annual tests and are required to undergo immediate remedial training if they fail to demonstrate appropriate

²⁶⁴ "Homeland Security Act of 2002" (P.L. 107-296, §425). The deadline was initially set for December 31, 2002 in the Aviation and Transportation Security Act, (P.L. 107-71 §110).

²⁶⁵ The Homeland Security Act ("Homeland Security Act of 2002" (P.L. 107-296, §425)) requires the Administrator of the TSA to report to Congress on the airports that are not electronically screening 100 percent of checked baggage, but these reports are classified. See also (a) Congressional Research Service, *Aviation Security: Issues before Congress Since September 11, 2001*. RL31969, (Washington: Congressional Research Service, June 18, 2003), 5; (b) Jeffrey Leib, "DIA Likely To Miss Screening Deadline," *Denver Post*, December 16, 2003, B1; and (c) Ron Marsico, "Airport Still Fails to Meet Bomb Rules," *The Star-Ledger*, January 1, 2004, 13.

²⁶⁶ GAO, *Aviation Security: Efforts to Measure Effectiveness and Strengthen Security Programs*, GAO-04-285T, (Washington: U.S. General Accounting Office, November 20, 2003).

²⁶⁷ GAO, *Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining*, GAO-03-1173, (Washington: U.S. General Accounting Office, September 24, 2003).

²⁶⁸ GAO, *Airport Security: Challenges to Airport Passenger and Baggage Screening*, GAO-04-440T, (Washington: U.S. General Accounting Office, February 12, 2004), 21.

screening techniques. It is unclear to what extent this training is meaningful, and whether the testing is a good indication of screener proficiency. According to the DHS Office of Inspector General:

“Newspaper articles reported that Transportation Security Administration (TSA) airport baggage screeners were given the answers to the questions prior to taking the final examination for certification.... TSA confirmed that 22 of the 25 questions on the final examination were the same as those used for daily lesson quizzes, concluded that the testing was conducted as prescribed by TSA, and found no misconduct on the part of the instructors....“When the OIG learned of TSA’s conclusions, we initiated our own review. **We were disturbed to learn that the screeners had, in fact, been given the answers to the final examination beforehand and to learn that TSA saw nothing wrong with this.** Our review confirmed that many of the final examination questions were identical or similar to questions that were given to the examinees in practice examinations. Furthermore, we found that many of the answers to the questions were obvious. **Accordingly, there could be no assurance from the testing program that the examinees had been trained to identify explosive devices in checked baggage.** In response to the OIG report, TSA promises to revise its testing program. The OIG will monitor this and undertake a complete review of TSA’s testing and training programs.”²⁶⁹ (emphasis added)

According to GAO, “TSA has deployed basic and remedial screener training programs, but has not fully developed or deployed a recurrent or supervisory training program to ensure that screeners are effectively trained and supervised.”²⁷⁰ Furthermore, supervisors that oversee screening operations have not necessarily undergone basic screening training themselves. As GAO notes, “TSA encourages, but does not require, screening managers, who are responsible for overseeing screening functions to participate in classroom training, even if they do not have prior screening experience.”²⁷¹ The TSA has recently begun identifying appropriate training programs, but will not have a fully trained supervisory workforce at the nation’s airports for several months at minimum.

By law,²⁷² five airports were designated by TSA to have non-federal screener workforces to serve as a basis for comparison after two years of TSA operations. Training at these non-TSA screener airports has been problematic. Under this program, airports and private screening services must meet the same overall hiring, training and security requirements as federal screeners.²⁷³ However, the security directors at these airports have struggled to get training products from TSA, hindering security and making comparisons of security at these and other airports difficult. According to officials with McNeil Security, the company providing security for Rochester International Airport, “[i]t is a fact that while numerous wait time surveys have been conducted

²⁶⁹ Department of Homeland Security Office of Inspector General. Semiannual Report to the Congress, April 1, 2003 – September 30, 2003, 5.

http://www.dhs.gov/interweb/assetlibrary/OIG_Fall_2003_SAR.pdf.

²⁷⁰ GAO, *Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining*, GAO-03-1173, (Washington: U.S. General Accounting Office, September 24, 2003), 2.

²⁷¹ GAO, *Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining*, GAO-03-1173, (Washington: U.S. General Accounting Office, September 24, 2003), 7.

²⁷² “Aviation and Transportation Security Act” (P.L. 107-71 §108).

²⁷³ Testimony of John Demill, President, Firstline Transportation Security. U.S. House, Committee on Government Reform, *Knives, Box Cutters, and Bleach: a Review of Passenger Screener Training, Testing, and Supervision* Hearing, November 20, 2003.

and there has been little or no recurrent training provided except which McNeil Security provided. Screening supervisors are giving no additional training beyond the basic screen training course It is not possible to identify those areas where screeners may need additional training. Screeners were supposed to be ranked by their test performance [during TSA inspections]. This is important information for corporate actual performance reviews. To date, this information has not been provided.”²⁷⁴

SECURITY RECOMMENDATION

Taken together, these cases demonstrate, at best, a lack of attention to appropriate screener and supervisor training. The TSA should ensure that every screener and supervisor is subject to, and demonstrates mastery over, all TSA screening procedures. The TSA and DHS should conduct routine tests at multiple airports to ensure that training is conducted appropriately and that active screeners are applying the training adequately. All screeners and supervisors should have rigorous recurrent training on an annual basis that consists more than cursory tests of routine screening procedures.

SECURITY GAP: Unscreened Air Cargo on Passenger Aircraft and Air Cargo Flights Remains Vulnerable to Exploitation.

Air cargo – freight, packages, and mail carried aboard passenger or all-cargo aircraft – continues to be a major security shortcoming. Roughly 2.8 million tons of cargo is transported by passenger planes annually, constituting 22 percent of all air cargo.²⁷⁵ Terrorists have previously exploited the lack of security in packages carried on planes: a device in a baggage container of Pan Am Flight 103 exploded on December 21, 1988, over Lockerbie, Scotland;²⁷⁶ and the FBI determined that an explosion aboard a November 15, 1979, U.S. airliner was caused by a parcel shipped by U.S. mail as air cargo, linked to the “Unabomber” Theodore Kaczynski.²⁷⁷ The TSA officials have determined that the risk of a terrorist bomb in air cargo has increased because the federal government is focused almost exclusively on screening passengers and luggage. According to a media characterization of a TSA report, “[c]argo is likely to become – and may already be – the primary threat vector in the short term.”²⁷⁸ There is a 35 percent to 65 percent likelihood that terrorists are planning to put a bomb in cargo on a passenger plane, another TSA document said, citing year-old intelligence reports.²⁷⁹

²⁷⁴ U.S. House, Committee on Government Reform, *Knives, Box Cutters, and Bleach: a Review of Passenger Screener Training, Testing, and Supervision* Hearing, November 20, 2003.

²⁷⁵ GAO, *Aviation Security: Efforts to Measure Effectiveness and Strengthen Security Programs*, GAO-04-285T, (Washington: U.S. General Accounting Office, November 20, 2003), 20.

²⁷⁶ See GAO, *Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System*, GAO-03-344, (Washington: U.S. General Accounting Office, December 20, 2002), Appendix I: Air Cargo Incidents and Follow-Up Actions, 22.

²⁷⁷ Affidavit of Assistant Special Agent in Charge, Terry D. Turchie, Before the U.S. District Court, District of Montana, April 3, 1996.

²⁷⁸ Greg Schneider, “Terror Risk Cited For Cargo Carried On Passenger Jets; 2 Reports List Security Gaps,” *Washington Post*, June 10, 2002, A1.

²⁷⁹ *Ibid.*

The Administration requested no dedicated funds for air cargo in its the fiscal year 2004 budget, but Congress provided \$85 million for this need. The Administration's fiscal year 2005 budget request does not include any increase over the \$85 million level funded in 2004.²⁸⁰

Despite the clear threat and a legal mandate to provide for the screening of all cargo carried on passenger aircraft,²⁸¹ TSA instead relies on random inspections and a "known shipper program" that has been shown to have several security shortcomings.²⁸² No cargo can be placed aboard a passenger aircraft unless the sender is a participant in the "known shipper" program, and those shippers are required to follow a set of security practices prescribed by TSA. However, TSA does not verify compliance with security regulations for all "known shipper" companies.²⁸³ In cases where verification is done, "TSA inspectors have found numerous security violations made by freight forwarders and air carriers during routine inspections of their facilities."²⁸⁴ Further, "Employees of shippers and freight forwarders are not universally subject to a background check."²⁸⁵ Moreover, no air cargo, including U.S. mail, weighing less than 16 ounces is screened or subject to any other security measures.²⁸⁶ Former TSA Administrator and current DHS Deputy Secretary, Admiral James Loy, testified in 2002 that "it is absolutely an imperative that we spend focused attention on getting a better approach to cargo. We have strengthened the known shipper program from what it used to be, but I do believe that it's still simply not enough [W]e must reach to [secure] cargo better."²⁸⁷

Department of Homeland Security officials have stated that, "Analysis performed by Battelle Corporation on behalf of FAA in 2001 determined that only a small percentage of the nation's air cargo could be physically screened efficiently with the available technology without significantly impeding the supply chain. Furthermore, because of significant technology limitations, there is

²⁸⁰ U.S. Department of Homeland Security, *Department of Homeland Security Transportation Security Administration Fiscal Year 2005 Congressional Budget Justification*, (Washington: Department of Homeland Security, February 2, 2004), 47-49.

²⁸¹ "Aviation and Transportation Security Act" (P.L. 107-71 §110).

²⁸² See, for example, (a) GAO, *Transportation Security: Federal Action Needed to Help Address Security Challenges*, GAO-03-843, (Washington: U.S. General Accounting Office, June 30, 2003), 23; (b) GAO, *Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System*, GAO-03-344, (Washington: U.S. General Accounting Office, December 20, 2002); and report of the TSA Aviation Security Advisory Committee, October 1, 2003.

<http://www.tsa.gov/public/display?theme=44&content=090005198005906d>.

²⁸³ For fiscal year 2004, Congress provided funds for 100 TSA inspectors "to perform more in-depth audits of shipper compliance with the known shipper requirement." House Report 108-280 accompanying the Department of Homeland Security Appropriations Act of Fiscal Year 2004. The Administration's budget request for fiscal year 2005 includes the same funding level for inspection of known shipper compliance. U.S. Department of Homeland Security, *Department of Homeland Security Transportation Security Administration Fiscal Year 2005 Congressional Budget Justification*, (Washington: Department of Homeland Security, February 2, 2004), 47-49.

²⁸⁴ GAO, *Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System*, GAO-03-344, (Washington: U.S. General Accounting Office, December 20, 2002), 8.

²⁸⁵ GAO, *Transportation Security: Federal Action Needed to Help Address Security Challenges*, GAO-03-843, (Washington: U.S. General Accounting Office, June 30, 2003), 23.

²⁸⁶ This exemption is significant as the explosive device used in Pan Am flight 103 is estimated to have weighed approximately 16 ounces. The explosive brought on board by Richard Reid is also estimated to have weighed less than one pound.

²⁸⁷ U.S. Senate, Committee on Commerce, Science and Transportation, *Status of Aviation Security One Year After September 11* Hearing, September 10, 2002.

no practical way to achieve 100 percent manual screening/inspection of air cargo.”²⁸⁸ As a result of this claim, based on a study conducted before September 11, 2001, Congress did not enact legislation that would have required 100 percent screening of air cargo on passenger aircraft.²⁸⁹ One reason given is that detection systems, such as the VACIS machine used to screen containers at seaports, are not sufficiently sensitive to identify the relatively small amounts of explosives needed to cause major damage to an aircraft.²⁹⁰ Secretary Tom Ridge, however, has indicated that the technology exists to screen all cargo.²⁹¹

Rather than screening all cargo, TSA has announced plans to screen all “high-risk” cargo in the future. However, TSA has little experience or expertise in determining risk and intends to benefit from the experience built by the Bureau of Customs and Border Protection (CBP).²⁹² Unfortunately, CBP’s risk assessment process is problematic. According to GAO, “while CBP’s strategy incorporates some elements of risk management, it does not include other key elements, such as a comprehensive set of criticality, vulnerability and risk assessments that experts told GAO are necessary to determine risk and the types of responses necessary to mitigate that risk. Also, CBP’s targeting system does not include a number of recognized modeling practices, such as subjecting the system to peer review, testing and validation.”²⁹³

SECURITY RECOMMENDATION

The TSA should provide adequate security for air cargo, with the ultimate goal of 100 percent inspection as soon as possible. The “known shipper” program should be strengthened by regularly verifying that all participating companies are following all security procedures,

(Continued on following page)

²⁸⁸ Letter from Asa Hutchinson, Under Secretary for Border and Transportation Security, to Senator Thad Cochran, July 8, 2003.

²⁸⁹ The U.S. House of Representatives passed the Homeland Security Appropriations Act for Fiscal Year 2004 with an amendment requiring complete screening of cargo transported on passenger planes. The Senate, following the letter from Under Secretary Hutchinson to Senator Thad Cochran, Chairman of the Senate Appropriations Subcommittee on Homeland Security, did not include such a requirement. The enacted legislation required only that “The Secretary of Homeland Security is directed to research, develop, and procure certified systems to inspect and screen air cargo on passenger aircraft at the earliest date possible: *Provided*, that until such technology is procured and installed, the Secretary shall take all possible actions to enhance the known shipper program to prohibit high-risk cargo from being transported on passenger aircraft.” “Department of Homeland Security Appropriations Act of Fiscal Year 2004” (P.L. 108-90 §521).

²⁹⁰ Presentation to House Select Committee on Homeland Security staff by TSA, January 15, 2004.

²⁹¹ During the question period of a hearing of the House Select Committee on Homeland Security, Representative Ed Markey stated “...technology exists. The only question is, how much money are you willing to spend on it? The technology is there that can screen the cargo.” Secretary Ridge responded, “That’s exactly right.” U.S. House, Select Committee on Homeland Security, *How is America Safer: A Progress Report on the Department of Homeland Security* Hearing, May 20, 2003

²⁹² TSA, “Air Cargo Strategic Plan,” November 2003.

²⁹³ <http://www.tsa.gov/public/display?theme=44&content=0900051980069bfe>.

GAO, *Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers*, GAO-04-325T, (Washington: U.S. General Accounting Office, December 16, 2003), ii.

perhaps through third parties inspections.²⁹⁴ The TSA should deploy similar detection equipment as is currently used for airline baggage,²⁹⁵ U.S. mail, and large shipping containers to inspect cargo on passenger planes while continuing to develop better technology options. Where electronic screening is currently impossible, other detection methods, including canine screening and hand searches, should be used as an interim solution.

- **All-Cargo Aircraft**

In addition to securing cargo on passenger planes, all-cargo aircraft are also at risk of terrorist attack. These aircraft, which are as large as passenger planes, could be hijacked and used as missiles. For this reason, TSA has limited passengers on these planes to those necessary for the flight and delivery of cargo, and requires that cargo planes either have hardened cockpit doors or meet alternate security measures.²⁹⁶ However, all-cargo aircraft that overfly the United States without landing are not subject to these security measures. This loophole is especially significant as DHS has cited intelligence that terrorists are seeking weaknesses in international flights.²⁹⁷

SECURITY RECOMMENDATION

TSA should extend security measures, including hardening cockpit doors and limiting non-essential passengers, to all cargo aircraft that overfly the United States.

SECURITY GAP: Passenger Aircraft are Vulnerable to Missile Attack.

The threat to commercial aviation from shoulder-fired missiles is immediate and severe. Terrorists have demonstrated an interest in using such “man portable air defense systems” (MANPADS),²⁹⁸ have possession or access to them, and face no significant defense against the proven efficacy of missile attack. For example, on August 12, 2003, Hemant Lakhani was arrested in Newark, New Jersey, after trying to sell a shoulder-fired missile to a Federal Bureau of Investigation (FBI) operative posing as an extremist who wanted to shoot down a commercial airplane. On November 28, 2002, terrorists fired two SA-7 MANPADS at an Israeli charter jet departing Mombasa, Kenya. Terrorists with links to al Qaeda were recently arrested in Hong Kong when attempting to purchase MANPADS from undercover FBI agents.²⁹⁹ The use of shoulder-fired missiles is widespread in attacks against military aircraft – it has been estimated

²⁹⁴ “According to TSA officials, in 1999 FAA requested funds to conduct a feasibility study on a system of third-party inspections, but the study was not funded by the Congress.” GAO, *Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System*, GAO-03-344, (Washington: U.S. General Accounting Office, December 20, 2002), 9.

²⁹⁵ As recommended by the Gore Commission and the Cargo Working Group. See GAO, *Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System*, GAO-03-344, (Washington: U.S. General Accounting Office, December 20, 2002), 12.

²⁹⁶ See 14 CFR - CHAPTER I - PART 129 §129.28 Flightdeck security. Some cargo planes do not have cabins that would allow a cockpit door, and are instead required to meet TSA-approved alternate security measures.

²⁹⁷ Statement of Secretary Tom Ridge upon raising of the terrorist threat level, December 21, 2003.

²⁹⁸ MANPADS also include classes of shoulder-fired missiles (SAMs).

²⁹⁹ See, for example, Ralph Vartabedian, “U.S. Officials Announce 2 Terrorism Indictments,” *Los Angeles Times*, November 7, 2002, 5.

that man-portable missiles caused 90 percent of worldwide combat aircraft losses from 1984-2001,³⁰⁰ and they have been used against aircraft using Baghdad International Airport during and after Operation Iraqi Freedom in Iraq.

Estimates of the global inventory of man portable missiles range from 250,000 to 700,000 systems, and they are available at reasonably low cost.³⁰¹ Some estimate that 27 militia groups and terrorist organizations possess such weapons.³⁰²

Due to the widespread availability and small size of shoulder-fired missiles, there can be no guarantee that they will be kept out of the United States or away from foreign destinations of U.S. air carriers. Due to the missiles' reasonably long range, they can be fired at airplanes from substantial distances away from airports, making airport perimeter security alone an insufficient defense.

The DHS has begun a two year, \$121 million program to investigate countermeasure technologies for missile attacks.³⁰³ The Science and Technology Directorate has established a Counter-MANPADs Special Program Office for this purpose and plans to investigate both adapting existing technologies from military aircraft defense systems and developing new technologies.

SECURITY RECOMMENDATION

The DHS should continue this research and development effort and should prepare plans for deploying missile countermeasure technologies onto passenger airplanes. Such plans should include options for deploying defenses on aircraft under heightened risk of attack, either because of the size of airplane or regular flight routes.

Additional steps should also be taken beyond missile countermeasures. Inspectors at TSA and Customs and Border Protection (CBP) should incorporate specific training for screeners and border inspectors to identify the missiles, and these agencies should work with counterparts overseas to do the same. State and local governments and law enforcement should be given additional guidance to help identify locations at high risk for missile firings, based on flight paths and location accessibility. Finally, the Administration should push to duplicate globally the

(Continued on following page)

³⁰⁰ Michael Puttre, "Facing the Shoulder-Fired Threat," *Journal of Electronic Defense*, April 1, 2001, No. 4, Vol. 24, 38.

³⁰¹ According to the Congressional Research Service "The missiles are about 5 to 6 feet in length, weigh about 35 to 40 pounds, and, depending on the model, can be purchased on the black market anywhere from a few hundred dollars for older models to upwards of almost a quarter million dollars for newer, more capable models. Shoulder-fired SAMs generally have a target detection range of about 6 miles and an engagement range of about 4 miles.... Published estimates on the number of missiles presently being held in international military arsenals range from 350,000 to 500,000..., estimates of shoulder-fired SAMs in terrorist hands vary considerably. Estimates range from 5,000 to 150,000 of various missile types." Congressional Research Service, *Homeland Security: Protecting Airliners from Terrorist Missiles, RL31741*, (Washington: Congressional Research Service, November 3, 2003), 1, 3, 4.

³⁰² Vivienne Walt, "Portable Missiles Concern Senators," *USA Today*, December 2, 2002, 1.

³⁰³ This includes \$60 million appropriated for fiscal year 2004 and \$61 million included in the President's request for fiscal year 2005.

recent agreement of the Asia Pacific Economic Group to “adopt strict domestic export controls on MANPADs; secure stockpiles; regulate MANPADs production, transfer, and brokering; ban transfers to non-state end users; and exchange information in support of these efforts.”³⁰⁴

SECURITY GAP: Unscreened Airport Employees and Vendors Can Gain Access to Secure Parts of Airports.

Congress has required that airport perimeters be secure, including the “screening or inspection of all individuals, goods, property, vehicles, and other equipment before entry into a secured area of an airport in the United States...” that will “assure at least the same level of protection as will result from screening of passengers and their baggage.”³⁰⁵ Yet, while TSA has spent billions of dollars to screen all passengers and flight crews traveling on U.S. passenger planes, it is TSA policy that airport workers may access sensitive locations without such checks.³⁰⁶ Thousands of vendor employees that work in airport terminals can bypass security screening once they have gone through a rudimentary background check and could potentially board an aircraft or give prohibited items to a passenger.

A similar security loophole exists for the workers that service the airplanes for food service, cleaning and maintenance, and loading cargo. The potential for harm in this system was demonstrated recently when 25 people, mostly current or former employees at John F. Kennedy Airport in New York were arrested for participating in a complex and long-running drug smuggling operation.³⁰⁷

Even more troubling, previous investigations have shown that unauthorized persons have been able to access airports and airplanes with false identification. The DHS Office of the Inspector General conducted testing in which unauthorized personnel were able “to gain access to the security checkpoints and consequently the sterile area of most of the airports tested.”³⁰⁸ In addition, TSA has found that hundreds of its own employees used false information on applications and job materials that allowed them to gain access to sensitive airport locations.³⁰⁹ Gaps in security at airport perimeters have also been documented. In one recent media account, journalists were able to gain access to the tarmac at large airports and could have reached passenger planes on the ground.³¹⁰

³⁰⁴ (a) The White House, “Fact Sheet: New APEC Initiatives on Counterterrorism,” October 21, 2003. <http://www.whitehouse.gov/news/releases/2003/10/20031021-4.html>; (b) Philip Shenon, “U.S. Reaches Deal to Limit Transfers of Portable Missiles,” *The New York Times*, October 21, 2003, A1.

³⁰⁵ “Aviation and Transportation Security Act” (P.L. 107-71 §106).

³⁰⁶ U.S. House, Committee on Homeland Security, *Identification Documents Fraud and the Implications for Homeland Security* Hearing, October 1, 2003

³⁰⁷ Robert F. Worth, “20 Airport Workers Held in Smuggling Of Drugs for Decade,” *The New York Times*, A1.

³⁰⁸ Department of Homeland Security, Office of Inspector General, “Fiscal Year 2004 Annual Performance Plan,” 23. http://www.dhs.gov/interweb/assetlibrary/FY2004_Performance_Plan.pdf.

³⁰⁹ GAO, *Aviation Security: Efforts to Measure Effectiveness and Strengthen Security Programs*, GAO-04-285T, (Washington: U.S. General Accounting Office, November 20, 2003), 18.

³¹⁰ Steve McVicker, “Local airports may have security flaws; Expert decries ‘easy access’,” *Houston Chronicle*, January 7, 2004, A1.

SECURITY RECOMMENDATION

The TSA should adopt policies to ensure that everyone with the potential to harm passenger airplanes is appropriately screened. Everyone and everything that reaches a part of the airport physically beyond the screening checkpoints should be required to undergo inspection. Similarly, anyone seeking to gain access to a sensitive or secure airport location should be required to present tamper-proof, biometric identification. Airport perimeters should also be made more secure, using a combination of physical defenses, surveillance, and patrols. The TSA should meet all of the requirements set in law for airport perimeter security.³¹¹

³¹¹ GAO, *Aviation Security: Efforts to Measure Effectiveness and Strengthen Security Programs*, GAO-04-285T, (Washington: U.S. General Accounting Office, November 20, 2003), 18-19.

**PROVIDING SECURITY
INSIDE AMERICA**

Protecting America's Critical Infrastructure

The infrastructures that form the backbone of the American economy, including transportation, energy, water, chemicals, telecommunications and computers, and the food supply, remain highly vulnerable to terrorist attacks. Even though al Qaeda has made clear its desire to conduct catastrophic attacks that cause mass casualties and severe damage to our economy, the Administration has done little since 9/11 to improve the security of our critical infrastructures. It has not conducted comprehensive national risk assessments to prioritize spending or protective measures, created incentives for the private sector to invest in security, or developed standards to assist in measuring progress toward more secure infrastructure. To close the massive security gaps presented by our critical infrastructure, the Administration must vigorously engage the private sector with a sense of urgency and seriousness that has not been present to date and be willing to use all the tools at its disposal – cooperation, incentives, and, if necessary, regulation – to achieve a significantly greater level of security for the American people.

Al Qaeda has made it clear that attacking critical infrastructures within the United States achieves its dual aims of taking American lives and disrupting our economy. Late in 2001, Osama bin Laden boasted that the combined effect of the attack on New York, was "no less than one trillion dollars." Other tapes purported to be from bin Laden claimed that, "The youths of God are preparing for you things that would fill your hearts with terror and target your economic lifeline."³¹²

While the United States has not suffered a terrorist attack since 9/11, the number of potential targets in the U.S. is nearly endless. For example, there are more than 7,000 U.S. chemical facilities where a toxic release could kill or injure over 10,000 people; an accident at any one of more than 120 of those facilities could threaten over one million people. The massive blackouts in the United States in August 2003, while not terrorism-related, demonstrated serious vulnerabilities in our electricity infrastructure. Transport systems of all sorts are particularly vulnerable to terrorist attack. The millions of rail and truck cars carrying toxic and combustible chemicals around the country daily are potential bombs on wheels. Every day, millions of citizens are potential targets at concentrated travel points like subway systems, train stations, and bridges and tunnels. Citizens are also vulnerable at concentrated public settings such as large buildings and public entertainment venues. Intelligence officials have warned of threats to water supplies and dams and of airplane attacks against nuclear facilities. Incidences of foot-and-mouth disease point out risks in the agricultural sector, while our ever-growing reliance on computers heightens the risk of cyberattacks.

³¹² Peter Bergen, "Al Qaeda's New Tactics," *The New York Times*, November 15, 2002, A31.

Selected Infrastructure or Key Assets³¹³	Asset Details
Agriculture and Food	87,000 food processing plants
Water	1,800 federal reservoirs; 1,600 municipal wastewater facilities
Public Health	5,800 hospitals
Telecommunications	Two billion miles of cable
Energy	2,800 power plants; 300,000 oil and natural gas producing sites; two million miles of pipelines
Transportation	120,000 miles of major railroads; 590,000 highway bridges; 500 major urban public transit operators; 5,000 public airports; 300 inland/coastal ports
Chemicals and Hazardous Materials	66,000 chemical plants, of which 12,000 are highly toxic and could put large numbers of Americans at risk in the event of terrorist caused release
Nuclear Power Plants	104 commercial nuclear power plants
Dams	80,000 dams
Large high volume structures	460 skyscrapers; 250 major arenas and stadiums

The Administration has not provided strong leadership to improve critical-infrastructure security. Indeed, according to The Brookings Institution, the Administration “largely ignores” major critical infrastructure in the private sector.³¹⁴ In testimony before the House Select Committee on Homeland Security (Select Committee), homeland security experts gave DHS “not a passing grade” on critical infrastructure protection.³¹⁵ In the area of critical infrastructure, the Administration is failing to adequately protect the homeland.

SECURITY GAP: Inadequate Incentives Exist to Promote Investments in Infrastructure Security.

To date, the extent of the Administration’s policy to protect critical infrastructures is a nearly singular reliance on voluntary private action.³¹⁶ While the private sector – which owns 85 percent

³¹³ The list provided here represents selected infrastructure sectors and key assets. Other sectors and assets include emergency services in 87,000 U.S. localities; 250,000 firms in 215 distinct industries in the defense industrial base; 26,600 FDIC insured banking and finance institutions; 137 million postal and shipping delivery sites; 5,800 historic monuments and buildings; and 3,000 government-owned and operated facilities.

³¹⁴ Michael O’Hanlon, Peter Orszag, Ivo Daalder, et al, *Protecting the American Homeland: One Year On*, (Washington, DC: The Brookings Institution, 2002, with a new preface, January, 2003), xiv.

³¹⁵ Peter Orszag, Senior Fellow, The Brookings Institution, “Critical Infrastructure Protection in the Private Sector: the Crucial Role of Incentives,” testimony before the House Select Committee on Homeland Security, joint hearing of the Subcommittee on Infrastructure and Border Security and the Subcommittee on Cybersecurity, Science, Research and Development, September 4, 2003.

³¹⁶ Office of Homeland Security, *National Strategy for Homeland Security*, (Washington, DC: the White House, July, 2002). According to the *National Strategy for Homeland Security*, private firms bear the primary responsibility for addressing public safety risks posed by their industries. See also, U.S. General

of critical infrastructure – must clearly play a crucial role in protecting critical infrastructures, “private markets by themselves do not provide adequate incentives to invest in homeland security.”³¹⁷ Ultimate responsibility to provide for the common defense rests with the federal government. Policies that rest on the assumption that the private sector will provide sufficient critical-infrastructure protection will fail to provide adequate protection against the threats we face in an age of global terrorism.

The Administration’s free-market approach to critical infrastructure is failing because, “the business of business is business, not homeland security,”³¹⁸ and, “current [private sector] efforts fall woefully short of what is required.”³¹⁹ Such shortcomings are acknowledged with respect to the chemical sector, for example. Secretary of Homeland Security Tom Ridge and former EPA Administrator Christine Todd Whitman both publicly voiced concern over the fact that chemical plants are attractive targets, stating that “voluntary efforts alone are not sufficient to provide the level of assurance Americans deserve,” and chemical facilities “must be required to take steps” to improve security.³²⁰

Security is a collective good; consequently, in a purely free-market system, businesses simply do not have the economic incentives to invest in the level of security that society requires. Furthermore, “The ability of certain sectors to raise the necessary capital [for security enhancements] may be limited,” and, “even sectors made up of large well capitalized firms are likely to make additional expenditures only if they can identify a net positive return on investment.”³²¹ As a result of such economic realities, to the extent that private initiatives have been undertaken, they have been piecemeal within industries and uneven across infrastructure sectors.

The Administration must use all the policy tools at its disposal to change the structure of incentives to increase the critical infrastructure security of the United States. According to The Brookings Institution economist Peter Orszag:

We must therefore alter the structure of incentives so that market forces are directed toward reducing the costs of providing a given level of security for the nation, instead of providing a lower level of security than is warranted.³²²

The need for using a full range of public policy tools, including incentives, is echoed by the GAO:

Accounting Office, *Homeland Security: Voluntary Initiatives are Under Way at Chemical Facilities, but the extent of Security Preparedness is Unknown*, GAO-03-439, March, 2003.

³¹⁷ Peter Orszag, Senior Fellow, the Brookings Institution, “Critical Infrastructure Protection in the Private Sector: the Crucial Role of Incentives,” testimony before the House Select Committee on Homeland Security, September 4, 2003.

³¹⁸ Michael O’Hanlon, Peter Orszag, Ivo Daalder, et al, *Protecting the American Homeland: One Year On*, (Washington, DC: The Brookings Institution, 2002, with a new preface, January, 2003), xiv.

³¹⁹ Ibid, xxi.

³²⁰ DHS Secretary Ridge and EPA Administrator Whitman, “A Security Requirement,” *Washington Post*, October 6, 2002, B6.

³²¹ Congressional Research Service, *Critical Infrastructures: Background, Policy, and Implementation*, May 6, 2003, 25.

³²² Peter R. Orszag, Senior Fellow in Economic Studies, the Brookings Institution, “Critical Infrastructure Protection in the Private Sector: the Crucial Role of Incentives,” testimony before the House Select Committee on Homeland Security, September 4, 2003.

Last year, the Comptroller General testified ... that the [DHS] would need to design and manage tools of public policy to engage and work constructively with third parties.... These [should] include grants, regulations, and tax incentives, and regional coordination and partnerships to motivate and mandate other levels of government or the private sector to address security concerns.... Without appropriate consideration of public policy tools, private sector participation in sector-related information sharing and other CIP efforts may not reach its full potential.³²³

The Administration's fiscal year 2005 budget request includes \$200 million for targeted infrastructure protection grants (no funding was included in the President's budget request for fiscal year 2004).³²⁴ Given the way in which such grants are currently used, however, the lasting benefits of such a program for increased infrastructure security are questionable. For example, of the \$200 million in infrastructure protection grants provided in the fiscal year 2003 supplemental appropriation, nearly all of the roughly \$60 million that has been spent to date went toward overtime pay for state and local law enforcement during the heightened terror alert before and during the Iraq War.³²⁵ While critically important, such activities are reactive and temporary and do not improve the security of facilities over the longer term. Furthermore, due to weak government tracking of the program, DHS has to date been unable to provide information on the distribution of grant spending by infrastructure sector.

SECURITY RECOMMENDATION

To increase critical infrastructure security to an acceptable level, the Administration should explore tax incentives that promote increased investments in security by owners of critical infrastructure; seek to speed the development of affordable commercial products – including terrorism insurance and security assessment and audit products – that can help business owners increase security and also defray the potential costs of terrorist attacks; and work with owners of critical infrastructure, as necessary, to ensure a minimum regulatory framework that helps promote security in each of the critical infrastructure sectors without placing unreasonable burdens on business owners.

Examples of minimum regulations include requirements that critical infrastructure owners: carry terrorism-related insurance; undertake periodic vulnerability assessments against industry-determined best practices; and undergo periodic security audits, with such audits performed by independent and qualified third parties and judged against established objective benchmarks. Such measures will not only enhance security but can contribute to improving the safety, reliability, and performance of America's infrastructure sectors. Constructive investments in critical infrastructure sectors could contribute to economic growth, help individual business owners improve the quality and safety of their facilities, and improve the quality and reliability of our infrastructure nationally.³²⁶ (continued on following page)

³²³ Robert Dacey, Director of Information Security Issues, General Accounting Office, written responses to posthearing questions from the September 17, 2003 hearing of the House Select Committee on Homeland Security, December 8, 2003.

³²⁴ Department of Homeland Security, "Budget in Brief: Fiscal Year 2005," February, 2004.

³²⁵ Office of Domestic Preparedness, briefing on the 2005 budget for members of the House Select Committee on Homeland Security, February 11, 2004.

³²⁶ See the American Society of Civil Engineers, *Report Card for America's Infrastructure, 2003 Progress Report*, September, 2003, <http://www.asce.org/reportcard> which grades the general non-security-specific quality of U.S. infrastructures. Energy infrastructure received a D+; roads and bridges a D+/C; transit a C-;

The Administration must also ensure that any current or future grant funding for infrastructure protection is guided by an overall strategy, has stronger mechanisms to account for how it is used, and is accompanied by a better understanding of what is truly needed to improve critical infrastructure security in both the near and long term.

SECURITY GAP: A Comprehensive Risk Assessment of Our Nation's Critical Infrastructures Still Has Not Been Completed.

Given the enormity of the task of securing our critical infrastructures, it is imperative to conduct a comprehensive risk assessment in order to identify our greatest vulnerabilities and prioritize the implementation of protective measures. Despite the crucial importance of this task, the Administration has made little progress in developing a comprehensive national critical-infrastructure risk assessment.

According to the 2002 Homeland Security Act, DHS is required to comprehensively assess critical infrastructure vulnerabilities, prioritize protective measures, develop a comprehensive national plan for securing critical infrastructures, and craft policy to protect critical infrastructure.³²⁷ Furthermore, the White House's *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* calls for DHS to identify key critical-infrastructure protection priorities and develop "an integrated critical infrastructure and key asset geospatial database."³²⁸

The potential risks of allocating limited homeland security resources in the absence of an informed risk assessment are apparent in the Transportation Security Administration's budget. In the fiscal year 2004 budget, 83.5 percent of the TSA budget was dedicated to aviation security, while only five percent went toward maritime and land transportation security.³²⁹ In the fiscal year 2005 budget request, spending on maritime and land transportation fell below three percent of TSA's budget.³³⁰ In the absence of a thorough and informed infrastructure risk assessment, we simply do not know whether such a disproportionate allocation of funds to aviation security makes sense. While aviation security should clearly be a priority, a full risk assessment might indicate that maritime and land transport deserve much greater attention. Trucks carry 68 percent, by weight, of all freight in the United States and they account for 82 cents on every dollar spent by U.S. businesses on shipping.³³¹ Furthermore, the National Intelligence Council

drinking water a D; wastewater a D; dams a D; and hazardous waste a D+. Infrastructure that is outdated and in poor condition is more vulnerable to potential disruption, terrorism-related or not.

³²⁷ Specifically, the Act, calls for DHS to: 1) Identify and assess the nature and threat of terrorist threats; 2) Understand such threats in light of actual and potential vulnerabilities; 3) Carry out comprehensive assessments of the vulnerabilities of key resources and critical infrastructure... including the performance of risk assessments to determine the risks posed by particular terrorist attacks within the U.S.; 4) Integrate relevant information, analyses, or assessments...in order to identify priorities for protective and support measures; 5) Develop a comprehensive national plan for securing key resources and critical infrastructures; and 6) To recommend measures necessary to protect the key resources and critical infrastructure

³²⁸ Office of Homeland Security, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, (Washington, DC: the White House, February, 2003), 24.

³²⁹ Congressional Research Service, "TSA Appropriations," memo to the House Select Committee on Homeland Security, November 4, 2003.

³³⁰ DHS briefing on the 2005 TSA budget request for members of the House Select Committee on Homeland Security staff, February 9, 2004.

³³¹ American Trucking Association at www.truckline.com. See also www.truckersbestfriend.com.

and leading homeland security experts view insecure ports and cargo containers as among the most likely means of weapons of mass destruction entering the United States.³³²

While the need for risk assessment as a crucial tool to prioritize efforts is widely accepted – even in the Administration’s own strategy documents³³³ – little has been done to perform the assessments. According to Governor James Gilmore, Chairman of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission), the Administration has written no less than eight homeland security strategies, and none of them were based on an adequate risk assessment.³³⁴ “The lack of a comprehensive assessment of threats to U.S. infrastructures hampers defensive measures and preparedness activities.”³³⁵ Furthermore, the conference report on the 2004 Homeland Security Appropriations Act requested that DHS develop a “comprehensive risk analysis and assessments of vulnerabilities” of critical infrastructures “on a national scale” that will “focus on problems affecting multiple infrastructures.”³³⁶ The report language directed the Department to provide, by December 15, 2003, a detailed program plan, including scope, cost, and schedule for completing the plan. Although both DHS Undersecretary for Information Analysis and Infrastructure Protection, Frank Libutti, and Assistant Secretary for Infrastructure Protection, Robert Liscouski, pledged in congressional testimony to meet that deadline,³³⁷ DHS has failed to deliver any plan to Congress. Instead, on December 17, the White House issued Homeland Security Presidential Directive 7 (HSPD-7), giving DHS yet another year to develop a ‘plan’ to develop a ‘strategy’ to identify, prioritize, and protect critical infrastructures. The Directive suggests that DHS is not getting the job done.

At a September, 2003 hearing before the Select Committee, testimony from DHS Assistant Secretary Liscouski cast serious doubt on whether the Administration is devoting adequate seriousness and attention to completing a comprehensive risk assessment in a timeframe that would allow such an assessment to inform critical programmatic and spending decisions.

³³² National Intelligence Council, *National Intelligence Estimate: Foreign Missile Developments and the Ballistic Missile Threat Through 2015*, (Langley, VA: Central Intelligence Agency, December, 2001). See also Steven Flynn, Senior Fellow, Council on Foreign Relations, “Potential Strange Bedfellows? Homeland Security and Non-Proliferation in the Post 9-11 World,” in *Monitor: International Perspectives on Nonproliferation*, September 18, 2003.

³³³ See Office of Homeland Security, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, (Washington, DC: the White House, February, 2003). See also Governor James Gilmore, “Perspectives on 9-11: Building Effectively on Hard Lessons,” testimony before the House Select Committee on Homeland Security, Sept 10, 2003.

³³⁴ Governor James Gilmore, “Perspectives on 9-11: Building Effectively on Hard Lessons,” testimony before the House Select Committee on Homeland Security, Sept 10, 2003.

³³⁵ Gilmore Commission, “Implementing the National Strategy,” Fourth Annual Report, (Arlington, VA: RAND, December 15, 2002), 84.

³³⁶ According to House Appropriations Committee Report 108-169 on HR 2555, the DHS “will also develop a comprehensive risk analyses on a national scale that will be cross-sector in nature and focus on problems affecting multiple infrastructures...the Committee directs the Department to provide a detailed program plan outlining the proposed scope, total estimated cost, and schedule for completing the comprehensive risk analysis and assessments of vulnerabilities or the critical infrastructure. This plan is to be provided to the Committee by December 15, 2003.”

³³⁷ Undersecretary Libutti, testimony on DHS’s Information Analysis and Infrastructure Protection Directorate, before the House Appropriations Committee, Subcommittee on Homeland Security, September 4, 2004. Assistant Secretary Liscouski, testimony on “Implications of Power Blackouts for the Nation’s Cybersecurity and Critical Infrastructure Protection: the Electric Grid, Critical Interdependencies, Vulnerabilities, and Readiness,” before the House Select Committee on Homeland Security, September 17, 2003.

CONGRESSWOMAN SANCHEZ: So you are telling me that in a month and a half, we are going to have a list with all of the very critical infrastructure sectors and where that infrastructure is, and what type of protection we need to do for it, or how we are going to protect and what it is going to cost us, and a prioritization of that list...

ASSISTANT SECRETARY LISCOUSKI: And I will shortly retire right after that too. No. I was really referring to the Liberty Shield list. The [list you refer to] is ...really a continuous work in progress, [the] assessment of all the critical infrastructure throughout the United States. I did not mean to mislead you to think that we would have all that categorized in the next month and a half. **I would be surprised, frankly, if we had that done in the next five years** *[emphasis added]*.³³⁸

Five years is too long to wait when the threats exist now. On February 23, DHS announced that it will create by December, 2004, a national database of all physical critical infrastructure, ranked by priority. This is a positive development, but is only the first step toward the development of a robust risk assessment that can be used to guide policy development and prioritize the allocation of resources to protect all of our vulnerable critical infrastructures.

SECURITY RECOMMENDATION

DHS, in coordination with the intelligence community, private sector experts, federally funded research and development centers and the national labs, should, as soon as possible, but not later than October, 2004, assemble an initial/draft national critical-infrastructure risk assessment. Such an assessment should include a full assessment of threats,³³⁹ vulnerabilities and consequences and leverage, to the fullest extent possible, already-existing risk assessments that have been performed by many states, infrastructure sectors and federal agencies. The study should be updated and improved on an annual basis. Funding for the risk assessment should be clearly identified in the President's annual budget with clear accountability for the assessment residing with DHS.

Congress should establish and the President support an expert advisory panel to assess critical-infrastructure security and suggest strategies for the protection of the nation's critical infrastructures.³⁴⁰

³³⁸ Assistant Secretary Liscouski, testimony on "Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection: the Electric Grid, Critical Interdependencies, Vulnerabilities, and Readiness," before the House Select Committee on Homeland Security, September 17, 2003.

³³⁹ Gilmore Commission, "Implementing the National Strategy," Fourth Annual Report, (Arlington, VA: RAND, December 15, 2002), iv, 47, 84. According to the report: 1) the President should direct that the National Intelligence Council perform a comprehensive National Intelligence Estimate on the threats to the nation's critical infrastructure; 2) DHS should produce continuing, comprehensive "strategic" assessments of threats inside the United States; 3) DHS should have a robust capability to combine threat and vulnerability information.

³⁴⁰ Ibid, 83.

SECURITY GAP: No Performance Critical Infrastructure Performance Metrics Have Been Developed to Measure Progress and Create Accountability.

According to the GAO, none of the Administration's homeland security strategies "indicates milestones" or "establishes performance measures" by which to measure or establish accountability for critical infrastructure protection.³⁴¹ Furthermore, according to the Gilmore Commission:

One of the critical shortcomings in structuring programs and securing funds to protect critical infrastructures is the lack of risk-based models and metrics to help explain the value of protective measures in terms that public and private decision makers understand.³⁴²

The Department includes only limited performance metrics regarding critical infrastructure in its fiscal year 2005 budget request. Specifically, DHS is seeking to increase the amount of threat information that it makes available to infrastructure sectors. By the end of 2005, DHS has set a 25 percent target for the number of infrastructure "assets" and "components" that will have "threat level information completed for use by decision makers for optimal deployment of assets."³⁴³ The initiative may mark positive movement toward measuring the Department's activities,³⁴⁴ but it falls far short of what is required, namely, specific risk-based models and metrics that fully incorporate threats, vulnerabilities and consequences and can be used to evaluate progress toward increased security within and across each of the critical infrastructure sectors.

SECURITY RECOMMENDATION

The Administration should follow the recommendation of the Gilmore Commission that DHS "develop metrics for describing infrastructure security in meaningful terms, and to determine the adequacy of preparedness."³⁴⁵ In this task, DHS should fully leverage the modeling and analytic capabilities of National Infrastructure Simulation and Analysis Center (NISAC) and work in concert with representatives from each of the critical infrastructure sectors.

The DHS should prepare an annual report card which assesses the state of preparedness of each of
(continued on following page)

³⁴¹ Robert Dacey, Director of Information Security Issues, General Accounting Office, written responses to posthearing questions from the September 17, 2003 hearing of the House Select Committee on Homeland Security, December 8, 2003.

³⁴² Gilmore Commission, "Implementing the National Strategy," Fourth Annual Report, (Arlington, VA: RAND, December 15, 2002), 85

³⁴³ DHS, "Performance Budget Overview, Fiscal Year 2005, Congressional Budget Justification," February, 2004.

³⁴⁴ Representative Christopher Cox (R, CA), Chairman of the House Select Committee on Homeland Security, has expressed interest in developing performance measures for DHS. See, for example, Office of Representative Cox, "Homeland Security Members Announce Performance Measures for the Department of Homeland Security," news conference and press release, November 19, 2003.

³⁴⁵ Gilmore Commission, "Implementing the National Strategy," Fourth Annual Report, (Arlington, VA: RAND, December 15, 2002), ix, 85.

the critical infrastructure sectors against specific performance metrics. In addition, DHS should grant annual awards recognizing significant improvements or achievements in critical-infrastructure protection. Such programs can be a powerful tool for government to motivate private sector actors to enhance infrastructure security, as the public-relations impact of such assessments can be significant.

SECURITY GAP: Information Sharing Between Government and Owners of Critical Infrastructure Needs to be Improved.

The improvement of information sharing between the federal government and owners of critical infrastructure is essential in securing the country against terrorist attacks. The government cannot adequately assess infrastructure vulnerabilities or respond to events without the essential input of infrastructure owners. Threat information must be bolstered by reports of suspicious incidents at individual facilities, and, in the event of an attack, infrastructure owners will be leading players in response and recovery. For the United States to adequately protect itself, communications between all levels of government and owners of critical infrastructures must be robust, full, and open.

The Administration has made little progress in achieving effective information sharing between all levels of government and private owners of critical infrastructure. Relationships between the private sector and the federal government are largely *ad hoc*, and the Administration needs to provide stronger leadership to make these relationships more explicit, more trusted, and more institutionalized.³⁴⁶

Specifically, the Administration has done little to delineate the functions, relationships, and mechanisms for information sharing in coordination with the critical sectors. According to the Partnership for Critical Infrastructure Security, the federal government has “not developed a comprehensive architecture describing the functions, relationships, and mechanisms for “information sharing” in coordination with the critical sectors.”³⁴⁷ The lack of progress on this front is disappointing, especially since both the GAO and the Gilmore Commission identified and have called for such measures since at least 2002.³⁴⁸ The GAO found that “none of the [levels] of

³⁴⁶ Kenneth C. Watson, President and Chairman, the Partnership for Critical Infrastructure Security, written responses to posthearing questions from the September 17, 2003 hearing of the House Select Committee on Homeland Security, November 17, 2003. Robert Dacey, Director of Information Security Issues, General Accounting Office, written responses to posthearing questions from the September 17, 2003 hearing of the House Select Committee on Homeland Security, December 8, 2003. Gilmore Commission, “Implementing the National Strategy,” Fourth Annual Report, (Arlington, VA: RAND, December 15, 2002).

³⁴⁷ Kenneth C. Watson, President and Chairman, the Partnership for Critical Infrastructure Security, written responses to posthearing questions from the September 17, 2003 hearing of the House Select Committee on Homeland Security, November 17, 2003.

³⁴⁸ Robert F. Dacey, the U.S. General Accounting Office, “Critical Infrastructure Protection: Significant Homeland Security Challenges Need to be Addressed,” statement of before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives, GAO-02-918T, July 9, 2002, 4, 20, 43. In particular, the GAO identified a number of critical infrastructure protection priorities, all of which implicate improved information and sharing and coordination: 1) Clear delineation of critical infrastructure protection roles and responsibilities for federal, state, local, and private sector actors; clarification of how critical infrastructure protection entities will coordinate their activities; 2) clear definition of interim objectives and milestones; 3) clear timeframes for achieving objectives; 4) establishment of performance metrics; 5) improvement in analytical and warning capabilities. See also, the

government perceived the current information-sharing process with the federal government to be effective... and the information that was shared was not perceived as timely, accurate, or relevant.”³⁴⁹

On February 19, 2004, the Administration released an interim final rule to protect information about the nation's critical infrastructure from public disclosure.³⁵⁰ It also created a critical infrastructure information office to receive voluntary information submissions from the private sector.³⁵¹ While these are positive steps, the rules are nearly two years late, as the Homeland Security Act required that such “procedures shall be established not later than 90 days after the date of enactment” of the Critical Infrastructure Information Act in January, 2002.³⁵² Furthermore, the ability of the rules to significantly improve information sharing remains unclear. Even if the new protections spur improved information flow from the private sector to DHS, the Department still lacks sufficient authority to require plant operators in vulnerable sectors to submit information or actually follow DHS advice and make security improvements. As a result, to significantly increase the level of information sharing “may also require the consideration of various public policy tools, such as grants, regulations, or tax incentives.”³⁵³

SECURITY RECOMMENDATION

The Administration must improve information sharing between government and owners of critical infrastructure. Specifically, the Administration should develop a comprehensive national plan to facilitate the sharing of critical-infrastructure information that clearly defines roles and responsibilities of the DHS, other federal agencies, state and local governments, and private owners of critical infrastructure before, during, and after an attack on critical infrastructures. As part of such a plan, comprehensive procedures for information sharing should be established and
(Continued on following page)

Gilmore Commission, “Implementing the National Strategy,” Fourth Annual Report, (Arlington, VA: RAND, December 15, 2002).

³⁴⁹ Robert Dacey, Director of Information Security Issues, General Accounting Office, written responses to posthearing questions from the September 17, 2003 hearing of the House Select Committee on Homeland Security, December 8, 2003. See also GAO, *Homeland Security Efforts to Improve Information Sharing Need to be Strengthened*, GAO-03-760, August 27, 2003.

³⁵⁰ The new regulations, promulgated under the 2002 Critical Infrastructure Information Act, are designed to address those fears by introducing an exemption from the freedom of Information Act. To qualify for the exemption, information about critical infrastructure must meet three criteria: it must be submitted by companies voluntarily; it must be information that they would not otherwise have to disclose to the government; and it must meet what the department calls ‘the definition of critical infrastructure information in the act and the implementing rule.’

³⁵¹ Assistant Secretary Liscouski, testimony on “Implications of Power Blackouts for the Nation’s Cybersecurity and Critical Infrastructure Protection: the Electric Grid, Critical Interdependencies, Vulnerabilities, and Readiness,” before the House Select Committee on Homeland Security, Subcommittee on Infrastructure and Border Security and the Subcommittee on Cybersecurity, Science, and Research and Development, September 17, 2003.

³⁵² The Critical Infrastructure Information Act of 2002 within the Homeland Security Act of 2002, P.L. 107-296, Title II, Subtitle B, sections 211-215.

³⁵³ Robert Dacey, Director of Information Security Issues, General Accounting Office, written responses to posthearing questions from the September 17, 2003 hearing of the House Select Committee on Homeland Security, December 8, 2003.

include the possible restructuring of interagency mechanisms.³⁵⁴

Additionally, the Administration should expand the Homeland Security Operations Center (HSOC) within DHS's IAIP Directorate to include on-site private-sector representatives from all major critical infrastructure sectors. Such inclusion of industry representatives will allow the HSOC to serve as a focal point for cooperation, trust-building, and education between and among critical infrastructure sectors and all levels of government.³⁵⁵

Finally, the Administration should create a new regime for security clearances that allows classifications for dissemination of intelligence and other information to private sector owners of critical infrastructure. A related training program for private sector officials to interpret intelligence products should be developed.³⁵⁶

³⁵⁴ Ibid. Gilmore Commission, "Implementing the National Strategy," Fourth Annual Report, (Arlington, VA: RAND, December 15, 2002). Gilmore Commission, "Forging America's New Normalcy: Securing Our Homeland, Protecting Our Liberty, Fifth Annual Report, (Arlington, VA: RAND, December 15, 2003).

³⁵⁵ Guy Copeland, Vice President, Information Infrastructure Advisory Programs, Computer Sciences Corporation and former Co-Chair, National Information Infrastructure Task Force, interview with House Select Committee on Homeland Security staff. Similarly, see the Gilmore Commission, "Forging America's New Normalcy: Securing Our Homeland, Protecting Our Liberty, Fifth Annual Report, (Arlington, VA: RAND, December 15, 2003), 16. which highlights the importance of significant and permanent state, local, and private sector representation within homeland security bodies responsible for intelligence assessment and incident management.

³⁵⁶ Gilmore Commission, "Forging America's New Normalcy: Securing Our Homeland, Protecting Our Liberty, Fifth Annual Report, (Arlington, VA: RAND, December 15, 2003), 33.

Protecting Chemical Plants

Across the nation, chemical facilities remain unsecured despite their clear vulnerability as terrorist targets. Reports of poor security and a pervasive lack of uniform standards and oversight mean that millions of Americans may be needlessly vulnerable to catastrophic terrorist attacks. Strong legislation must be adopted quickly that will build an effective public-private partnership for assessing the vulnerability and increasing the security of chemical facilities, both in the near and long term.

The United States is home to more than 66,000 chemical production and storage facilities spread throughout our cities, towns, and rural areas. These facilities are essential components of the economy, providing crucial support to U.S. manufacturing, agricultural, and energy sectors, producing valuable products for export, and employing more than one million workers.³⁵⁷ But chemical plants are also tempting terrorist targets.

Catastrophic releases from facilities that store large quantities of toxic and hazardous materials threaten serious harm to nearby residents and property and could produce severe economic disruption. A 2002 Brookings Institution report ranks an attack on a chemical facility second only to biological and nuclear attacks in terms of possible fatalities.³⁵⁸ As terrorism expert Jonathan Tucker points out, “hazardous chemicals are ubiquitous in modern industrial society and hence are more accessible to terrorists than either biological or fissile material.”³⁵⁹ Mandatory industry reporting to the Environmental Protection Agency (EPA) indicates that any of 123 facilities in the U.S. could threaten more than one million people in the event of a massive breach of chemical containment,³⁶⁰ while over 7,000 facilities endanger up to ten thousand people.³⁶¹ In 2001, the Army surgeon general suggested that an attack on a chemical plant in a densely populated area could result in up to 2.4 million casualties.³⁶² The most relevant past experience, the devastating release of a toxic gas cloud from a chemical plant in Bhopal, India in 1984, killed at least 4,000 people and injured an estimated 400,000.³⁶³ Finally, chemicals stored at such sites present a ready source of dangerous material that could be stolen and deployed elsewhere by terrorists.³⁶⁴

³⁵⁷ American Chemistry Council, *Protecting a Nation: Homeland Defense and the Business of Chemistry*, April 2002.

³⁵⁸ Michael O’Hanlon and others, *Protecting the American Homeland: A Preliminary Analysis*, (Washington, D.C.: Brookings Institution Press, 2002): 47.

³⁵⁹ Jonathan B. Tucker, “Chemical Terrorism: Assessing Threats and Responses,” *High Impact Terrorism: Proceedings of a Russian-American Workshop*, (Washington, D.C.: National Academy Press, 2002): 117.

³⁶⁰ Paul R. Kleindorfer, James C. Belke, Michael R. Elliott, Kiwan Lee, Robert A. Lowe, Harold I. Feldman, “Accident Epidemiology and the U.S. Chemical Industry: Accident History and Worst-Case Data from RMP*Info,” *Risk Analysis*, 23, no. 5, (2003): 865-881.

³⁶¹ Department of Justice, *Assessment of the Increased Risk of Terrorist or other Criminal Activity Associated with Posting Off-Site Consequence Analysis Information on the Internet*, (April 18, 2000): 13.

³⁶² Office of the Surgeon General, U.S. Army, *Draft Medical NBC Hazard Analysis of Chemical-Biological-Radiological-Nuclear-High Explosive Threat: Possible Scenarios and Planning Requirements*, (October 2001).

³⁶³ Dan Kurzman, *A Killing Wind: Inside Union Carbide and the Bhopal Catastrophe*, (New York: McGraw-Hill, 1987).

³⁶⁴ Congressional Research Service, *Chemical Plant Security*, RL31520, October 27, 2003.

As “soft” targets, chemical plants have traditionally remained unprotected against a possible terrorist attack. In November 2003, the television magazine *60 Minutes* reported unlocked gates, absent guards, dilapidated fences, and unprotected tanks filled with deadly chemicals at dozens of facilities in major metropolitan areas, including Chicago, Houston, New York, Los Angeles, and Baltimore.³⁶⁵ In the Pittsburgh area, one reporter found easy access to more than 200 tons of corrosive chlorine gas at four different sites.³⁶⁶ Some industrial security experts have described industry’s recent claims of improved security as “window-dressing” and “exaggerated.”³⁶⁷ Based on these reports, it is reasonable to assume that security lapses exist at many U.S. chemical facilities.

Administration officials themselves have pointed to chemical facilities as vulnerable and likely terrorist targets. Soon after September 11, the Administration directed agencies such as the EPA to remove web-based information about chemical plants that could prove useful to terrorists.³⁶⁸ In February, 2003, the Administration warned that terrorists “may attempt to launch conventional attacks against U.S. nuclear/chemical industrial infrastructure to cause contamination, disruption and terror.”³⁶⁹ As recently as this past holiday season, Department of Homeland Security (DHS) officials warned of possible targeting of chemical plants by terrorists.³⁷⁰ The Justice Department has described the threat to chemical plants as “both real and credible” and potentially more dangerous than an attack on a nuclear power plant.³⁷¹ Over a year ago, DHS Secretary Tom Ridge and former EPA Administrator Christine Todd Whitman both publicly voiced concern over the fact that chemical plants are attractive targets, stating “voluntary efforts alone are not sufficient to provide the level of assurance Americans deserve” and chemical facilities “must be required to take steps” to improve security.³⁷²

Today, these statements have not been translated into firm, effective measures to secure our nation’s chemical facilities. In the 28 months since September 11, 2001, the Administration has taken only “preliminary steps” towards ensuring the security of these vulnerable facilities.³⁷³ Two independent assessments have given the Administration a “D” grade on chemical plant security.³⁷⁴ Meanwhile, the vulnerability of chemical plants remains largely unassessed and unaddressed.

³⁶⁵ “U.S. Plants: Open for Terrorists,” *60 Minutes*, broadcast November 16, 2003.

³⁶⁶ Carl Prine, “Chemical Sites Still Vulnerable,” *Pittsburgh Tribune-Review*, November 16, 2003.

³⁶⁷ (a) Jeanne Meserve, “Chemical Plants: Are They Safe from Terrorist Attacks?” *Wolf Blitzer Reports-Cable Network News*, broadcast November 17, 2003; (b) Adam Fifield, “How to Reduce Risks of Toxic Disaster” *Philadelphia Inquirer*, April 21, 2003, A1.

³⁶⁸ “Agencies Censor Sites Deemed Useful to Terrorists,” *Associated Press*, October 12, 2001.

³⁶⁹ Margaret Kriz, “Security Leak,” *National Journal*, August 2, 2003, 2476.

³⁷⁰ U.S. Department of Homeland Security, “Statement by the Department of Homeland Security on Continued Al-Qaeda Threats,” November 21, 2003.

³⁷¹ James V. Grimaldi and Guy Gugliotta, “Chemical Plants Feared as Targets,” *Washington Post*, December 16, 2001, A1.

³⁷² Thomas Ridge and Christine Todd Whitman, “A Security Requirement,” *Washington Post*, October 6, 2002, B6.

³⁷³ U. S. General Accounting Office, *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness is Unknown*, GAO-03-439, (Washington, D.C.: GAO, March 2003): 18.

³⁷⁴ (a) Progressive Policy Institute, *America at Risk: A Homeland Security Report Card*, July 2003, 19, http://www.ppionline.org/documents/HomeSecRptCrd_0703.pdf; (b) Neil Munro and Margaret Kriz, “National Security: Hardening the Targets,” *National Journal*, August 10, 2002, 2388.

SECURITY GAP: There Has Been No Comprehensive Assessment of Chemical Facility Vulnerabilities.

In March 2003, the General Accounting Office (GAO) issued a major report pointing out that the lack of chemical plant vulnerability assessments means the extent of security preparedness at U.S. chemical facilities is unknown.³⁷⁵ This situation is a direct result of the fact that chemical facilities are not required to assess their own vulnerabilities. For those facilities that have conducted assessments, no federal agency has the authority to set standards or review their actions. This information is crucial if the DHS is to carry out its legislative requirement to produce comprehensive assessments of the vulnerabilities of critical infrastructure and integrate relevant information, analyses, and vulnerability assessments in order to identify priorities for protective and support measures.³⁷⁶ Without these assessments, facility operators, law enforcement and emergency responders may not be prepared to respond appropriately to security threats. The GAO recommended the immediate passage of legislation requiring chemical facilities to assess their vulnerability to terrorist attack. Almost a year later, legislative action remains stalled.

SECURITY RECOMMENDATION

Legislation must be passed that requires the identification of high-risk facilities and requires those facilities to conduct vulnerability assessments and submit these plans to the DHS. The Administration should adopt uniform standards for conducting these assessments. Vulnerability assessments should be reviewed by government officials so that a comprehensive assessment of chemical infrastructure vulnerability can be completed.

SECURITY GAP: There Are No Legal Requirements for Chemical Facilities To Improve Security.

The Administration has relied almost exclusively on voluntary industry efforts to remedy the glaring vulnerabilities of our nations' chemical facilities. The American Chemistry Council (ACC) and the Synthetic Organic Chemical Manufacturer's Association have adopted a "Security Code," which must be followed by association members,³⁷⁷ and the American Petroleum Institute has published *Security Guidelines for the Petroleum Industry*.³⁷⁸ While laudable, these industry actions have clearly not been sufficient, given recently reported security gaps at chemical facilities. Voluntary efforts such as these are not practiced by the entire industry, leaving thousands of vulnerable chemical plants without an obligation to make any security assessments or improvements. Although it is the largest industry association, ACC members own only 7% of the 15,000 potentially most hazardous facilities.³⁷⁹ In addition, membership and participation in

³⁷⁵ GAO, *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness is Unknown*, GAO-03-439, (Washington, D.C.: GAO, March 2003): 30.

³⁷⁶ Section 201 of the *Homeland Security Act of 2002*, codified in 6 U.S.C. 121(d).

³⁷⁷ Esther D'Amico, "Putting a Lid on Site Security," *Chemical Week*, July 2, 2003, 33.

³⁷⁸ American Petroleum Institute, *Security Guidelines for the Petroleum Industry*, Second Edition. (Washington, D.C.: API Publishing Services, April 2003).

³⁷⁹ GAO, *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness is Unknown*, GAO-03-439, (Washington, D.C.: GAO, March 2003): 27.

such voluntary programs fluctuates without any outside control or oversight. ACC recently lost three of its members, each an owner of dozens of chemical facilities that now are no longer covered by the association's "Security Code" program.³⁸⁰

The Administration has taken some steps towards addressing chemical security. The Department of Homeland Security announced that it "has visited several hundred facilities in high-threat urban areas,"³⁸¹ and that Department personnel "will continue to conduct site visits to assist operators and owners in identifying and reducing vulnerabilities."³⁸² However, DHS lacks the authority to require reluctant plant operators to actually follow the Department's advice and make security improvements. The Department also does not have the power to conduct mandatory inspections and oversee industry actions to ensure their sufficiency. According to the GAO, "no federal oversight or third-party verification ensures that voluntary industry assessments are adequate and that necessary corrective actions are taken."³⁸³ In the current environment, those facilities that do not invest in security improvements have a competitive advantage over those that are taking voluntary action. Because the risk of attack at any single facility is low, it makes economic sense for owners to avoid making security improvements. To level the playing field, industry leaders have called for "oversight, inspection, and strong enforcement authority at the Department of Homeland Security to ensure that facilities are secure against the threat of terrorism."³⁸⁴

SECURITY RECOMMENDATION

Chemical facilities should be required by DHS to develop security plans that address vulnerabilities identified in assessments, and to implement improvements and upgrades. Security plans, including cost estimates, should be submitted and reviewed by government officials to ensure compliance and provide oversight. Strong sanctions should be authorized to compel facilities not in compliance to expeditiously make security improvements. Furthermore, appropriate mechanisms for the pooling and sharing of information about security practices that do not compromise sensitive data should be established. The information DHS collects should be used by both government and industry to assist in constantly improving security strategies. The DHS must partner with EPA, with its expertise in chemical plant operations and hazardous materials handling, in order to strengthen requirements and oversight of security both outside and inside the plant gates.

SECURITY GAP: Chemical Facilities are Not Required To Consider Using Inherently Safer Technologies.

A recent paper by the National Pollution Prevention Roundtable, an organization of scientific and industrial experts, noted that "physical security measures are very much penetrable by those with

³⁸⁰ Anne Thayer, "ACC Convenes Amid Upheaval," *Chemical and Engineering News*, November 3, 2003, 10.

³⁸¹ The White House, "Fact Sheet: Progress in the War on Terror," press release, January 22, 2004, <http://www.whitehouse.gov/news/releases/2004/01/20040122-1.html>.

³⁸² "Department of Homeland Security," *Budget of the United States, Fiscal Year 2005*, (Washington, D.C.: GPO, 2005): 170.

³⁸³ GAO, *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness is Unknown*, GAO-03-439, (Washington, D.C.: GAO, March 2003): 30.

³⁸⁴ American Chemistry Council, "Chemical Industry Security: Much Progress Made But Security Lapses Unacceptable," press release, November 18, 2003.

intent and do not reduce the risk associated with the target of attack.”³⁸⁵ A different approach, one based on new science and technology, is required to truly reduce the attraction of industrial chemicals as weapons for terrorists. According to President Bush’s science and technology advisor, Dr. Jack Marburger, technologies that reduce the toxicity, flammability, or other hazardous characteristics of chemicals and their processes “help improve the environment, public health, and competitiveness, but they also inherently reduce the threat of terrorism.”³⁸⁶ Replacing dangerous chemicals and processes with “inherently safer technologies” (IST) will fundamentally diminish and possibly eliminate the danger posed by a chemical facility.³⁸⁷ Current examples include the use of bleach instead of chlorine gas for water treatment³⁸⁸ or the replacement of highly toxic and aerosolizable hydrogen fluoride in hydrocarbon alkylation with sulfuric or solid acid catalysis.³⁸⁹ For the future, numerous opportunities exist to develop new technologies in chemical processing³⁹⁰ and chemical design³⁹¹ to reduce the application of existing hazardous processes and materials. Ultimately, approaches such as these are the only way to remove these facilities from terrorists’ target lists.³⁹² But the Administration has opposed legislation requiring facilities to formally consider adopting IST where practicable³⁹³ and has systematically undermined the chemical security activities of the EPA, the only federal agency with expertise in IST.³⁹⁴ It has no strategy for developing what the National Research Council calls “safer, intrinsically secure, economically viable chemical processes and procedures.”³⁹⁵

SECURITY RECOMMENDATION

Chemical facilities should be required to consider adopting IST or other “alternative approaches” that can make a chemical or chemical process less hazardous while retaining cost-effectiveness. Even if these strategies are not adopted, information regarding the economic and technological barriers to its adoption to improve security should be collected and, with the leadership of EPA, an analysis undertaken that will identify opportunities across the industry where IST can improve security and investments can be made in research that will enhance IST and its adoption in the future.

³⁸⁵ National Pollution Prevention Roundtable, *White Paper on Pollution Prevention and Homeland Security*, February 11, 2004, http://www.p2.org/whitepapers/p2_and_homeland_security.doc.

³⁸⁶ Stephen Ritter, “Green Solutions to Global Problems,” *Chemical and Engineering News*, September 29, 2003, 33.

³⁸⁷ Commission on Physical Sciences, Mathematics, and Applications, *Frontiers in Chemical Engineering: Research Needs and Opportunities*, (Washington, D.C.: National Academies Press, 1988): 112-113.

³⁸⁸ James Grimaldi and Guy Gugliotta, “Chemical Plants Are Feared as Targets,” *Washington Post*, December 16, 2001, A1.

³⁸⁹ Meghan Purvis and Warren Claflin, *Needless Risk: Oil Refineries and Hazard Reduction*, (Washington, D.C.: USPIRG Education Fund, October 2003): 16-19; http://uspirg.org/reports/NeedlessRisk10_03.pdf.

³⁹⁰ Board on Chemical Science and Technology, *Beyond the Chemical Frontier: Challenges for Chemistry and Chemical Engineering*, (Washington, D.C.: National Academies Press, 2003): 33-40.

³⁹¹ Martin Poliakoff and others, “Green Chemistry: Science and Politics of Change,” *Science*, 297, (August 2, 2002): 807-810.

³⁹² Jeff Johnson, “Simply Safer,” *Chemical and Engineering News*, February 3, 2003, 23.

³⁹³ John Mintz, “Bush Seeks Voluntary Chemical Plant Security Steps,” *Washington Post*, April 8, 2003, A10.

³⁹⁴ (a) “Administration Moves to Limit EPA Role in Homeland Security Efforts,” *ChemicalPolicyAlert.com*, December 29, 2003; (b) Carl Prine “EPA’s Security Push Fails,” *Pittsburgh Tribune-Review*, July 14, 2002.

³⁹⁵ Committee on Science and Technology for Countering Terrorism, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, (Washington, D.C.: National Academy Press, 2002): 132.

Protecting Cyberspace

The most vital systems of our society are all dependent on technology and computers. As a nation, we are only as strong as the security on the weakest link on these interconnected and interoperable systems. A weak link can allow a hacker to open a dam, close down an air traffic control system, or create financial havoc for our banking industry. We must secure these weak links by building strong prevention, detection, and response mechanisms for addressing potential threats to our networks. If cybersecurity is not a priority, then our economy and our infrastructures are at risk. Government, the private sector, and academia should all work together to develop a culture of security in cyberspace.

According to a recent survey conducted by the Pew Internet and American Life Project, almost half of Americans fear terrorists will launch cyberattacks on our critical infrastructures, disrupting major services and crippling economic activity.³⁹⁶ These fears are not unwarranted; as during the past decade our critical infrastructures, military operations, business, and home networks have become interconnected and interdependent. These interdependencies, however, are neither well understood nor well mapped. In addition, our computer systems are global and connected to similar networks around the world. These connections create international challenges and underscore the need to work with other countries in securing their systems. The result of this increasing interdependency is that the threats to and vulnerabilities in our nation's cybersecurity are growing faster than we can address them.

It was only a few years ago that a computer hacker gained control of a telephone system and disabled the control tower of the Worcester, Massachusetts airport, shutting down the airport for more than six hours.³⁹⁷ Others have penetrated the computer systems of the California Independent System Operator, the nonprofit corporation that controls the distribution of 75 percent of the state's electricity, and the Roosevelt Dam in Arizona.³⁹⁸ In the latter case, it is believed that the intruder gained command of the system that controlled the dam's floodgates and 400 trillion gallons of water. If he had released the flood gates, there would have been widespread loss of life and damage to the towns downstream of the dam. Some communities, infrastructures, and our economy have already suffered from cyber attacks. For example, an individual gained access to a utility company computer in Australia in 2000, releasing millions of gallons of raw sewage into a Queensland community's waterways.³⁹⁹ Just this past summer, the

³⁹⁶ Pew Internet & American Life, *The Internet and Emergency Preparedness: joint survey with Federal Computer Week magazine*, August 31, 2003, <http://www.pewinternet.org/reports/toc.asp?Report=100>.

³⁹⁷ U.S. Department of Justice, "Juvenile Computer Hacker Cuts off FAA Tower At Regional Airport - First Federal Charges Brought Against a Juvenile for Computer Crime," press release, March 18, 1998, <http://www.usdoj.gov/criminal/cybercrime/juvenilepld.htm>.

³⁹⁸ U.S. Department of Justice, *Statement of Michael Chertoff, Assistant Attorney General, Criminal Division Before the Committee on the Judiciary, Subcommittee on Crime, U.S. House of Representatives*, June 12, 2001; see also Barton Gellman, "Cyber-Attacks by Al Qaeda Feared; Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say," *Washington Post*, June 27, 2002, Page A01.

³⁹⁹ *Ibid.*

Sobig computer virus temporarily shut down the 23,000-mile-long CSX rail system.⁴⁰⁰ Indeed, Sobig, along with the Blaster and Welchia viruses, caused more than \$32.8 billion in economic damages in August 2003 alone, according to mi2g, a digital risk assessment company based in London.⁴⁰¹ The damages caused by Mydoom-A, which struck computers worldwide the week of January 26, 2004, has yet to be undetermined, though we know that by January 27 it had infected one out of every 41 e-mail messages.⁴⁰²

SECURITY GAP: We Are Not Prepared for an Electronic “9-11.”

If an electronic 9-11 were to happen tomorrow, who in the government could coordinate the efforts of dozens of agencies and effectively reach out to the private sector, which owns 85 percent of our critical infrastructures? It is not clear who has the authority and capability within the federal government to bring together the various federal and state agencies, as well as the relevant private sector entities, in the event of a cyber-catastrophe.

In 1996, the United States government, recognizing the need for a comprehensive national strategy to protect cyberspace, created the first national effort to secure our networks.⁴⁰³ Among the entities created as a part of this strategy were the National Infrastructure Protection Center (NIPC), a multi-agency organization housed at the FBI that served as the focal point for coordinating government-wide cybersecurity and critical infrastructure response, and the Critical Infrastructure Assurance Office (CIAO), a Commerce Department entity tasked with developing national critical infrastructure protection plans and coordinating outreach, education, and awareness programs.⁴⁰⁴ These entities recognized the need to pool the resources of numerous agencies and engage the private sector in the country’s cybersecurity efforts.

Soon after September 11, 2001, the current Administration created the Critical Infrastructure Protection Board to coordinate and oversee federal efforts to protect the networks and systems of critical infrastructures, federal assets, and national security programs.⁴⁰⁵ The Board was comprised of senior governmental officials and chaired by Richard Clarke, who also served as special advisor to the President for cyberspace security and headed the White House Office of Cybersecurity.

Less than a year and a half after its creation, in April 2003, the Critical Infrastructure Board was dissolved.⁴⁰⁶ NIPC and CIAO have been eliminated, with some, but not all, of their former responsibilities transferred over to the Department of Homeland Security (DHS). Clarke, his deputy, and the top officials at NIPC and CIAO left the government, leaving many wondering

⁴⁰⁰ CSX Corp., “Computer Virus Strikes CSX Transportation Computers,” press release, August 20, 2003, http://www.csx.com/index.cfm?fuseaction=company.news_detail&i=45722&ws=corporation.

⁴⁰¹ Mi2g, <http://www.mi2g.com/>.

⁴⁰² John Hogan, “A week of gloom and Mydoom,” *searchwin2000.com*, January 30, 2004.

⁴⁰³ President, “Executive Order 13010—Critical Infrastructure Protection,” 61 *Fed. Reg.* 138, July 17, 1996.

⁴⁰⁴ President, “Presidential Decision Directive 63,” May 22, 1998.

⁴⁰⁵ President, “Executive Order 13231-Critical Infrastructure Protection in the Information Age,” 66 *Fed. Reg.* 53063, October 18, 2001.

⁴⁰⁶ Diane Frank, “Tritak departs CIAO, government,” *Federal Computer Week*, January 17, 2003, <http://www.fcw.com/fcw/articles/2003/0113/web-tritak-01-17-03.asp>; see also Dan Verton, “NIPC chief Ron Dick to retire,” *Computerworld*, December 9, 2002, <http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,76538,00.html>.

who was in charge of protecting our infrastructures⁴⁰⁷ and whether the Administration was dedicated to protecting the nation's cyber networks.⁴⁰⁸

Amid criticism from the private sector regarding the lack of attention being paid by the government to cybersecurity, DHS announced on June 6, 2003, the creation of the National Cyber Security Division (NCSD). With a requested budget of \$80 million for Fiscal Year 2005, the NCSD is tasked with coordinating the cybersecurity activities within DHS and other agencies and is to serve as the central point of contact for the private sector.⁴⁰⁹ It took three months for the Administration to find a director willing to lead NCSD. Concerns remain that the new director is buried too deep in the bureaucracy of DHS with little authority for effectively leading our country's cybersecurity efforts.⁴¹⁰ Additionally, the Director does not have the authority to direct the multiple agencies, at the senior level needed, in the event of a cyber incident.

The Administration, overall, has been moving too slowly on securing our computer networks. It has been more than a year since February 2003 when the Administration released its "National Strategy to Secure Cyberspace," which set forth five cybersecurity priority areas. Those areas included:

- The development of a cybersecurity response system;
- The creation of a threat and vulnerability reduction program;
- The creation of awareness and training programs;
- The unveiling of plans for securing government computers; and
- The development of plans detailing national security and international cooperation.

The Administration's efforts to implement the strategy are lagging, leaving our nation at risk and unprotected. Since the creation of the NCSD nine months ago, DHS has announced then eliminated cybersecurity initiatives such as the Cyber Security Tracking, Analysis, & Response Center (CSTARC), a unit designed to detect and response to Internet events, track potential threats and vulnerabilities, and coordinate incident response with federal, state, local, private sector, and international partners.

The agency also is just beginning to provide some of the services that were available in similar form prior to the reorganization that created the agency. In September 2003, DHS created the US-CERT program to aggregate available cyber security information and provide it to individuals and organizations in a timely and understandable manner. Many questions remain as to when the US CERT will be fully functioning, how it will work with the Information Sharing and Analysis Centers (ISACs) that are responsible for private sector information sharing initiatives, and how it will work with the private sector. To date, the initiatives announced by the US CERT appear to recreate, in part, programs that existed before DHS was created or duplicate private sector

⁴⁰⁷ Barton Gellman, "Anti-Terror Pioneer Turns In the Badge After 11 Years, Clarke Leaves Legacy of Lasting Change -- and Enemies," *Washington Post*, Page A21, March 13, 2003; *see also* William Jackson, "Howard Schmidt is Leaving the White House," *Government Computer News*, April 21, 2003, http://www.gcn.com/vol1_no1/daily-updates/21815-1.html.

⁴⁰⁸ "Uncertain Future for Cybersecurity? Now that PCIPB has been dissolved, Illena Armstrong questions how future initiatives will be led," *SC Magazine*, April 2003.

⁴⁰⁹ "Tech Industry Wants Cybersecurity Czar," *Foxnews.com*, April 23, 2003, <http://www.foxnews.com/story/0,2933,84865,00.html>.

⁴¹⁰ Dan Verton, "A major DHS cybersecurity post remains vacant," *Computerworld*, July 21, 2003, <http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,83242,00.html>.

initiatives. These programs do not bring the nation much further on securing our computer networks than we were two years ago when NIPC, CIAO, and other entities existed.

For example, DHS announced in January that the NCSD, through US CERT, would begin producing several new “products” to inform individual computer users and security professionals about cyberthreats via e-mail. This announcement came a day after the Mydoom-A virus struck our nation’s computers. These products, in part, seem to replicate initiatives that existed at NIPC. Technical users can now receive “summaries of security issues, new vulnerabilities, potential impact, patches and work-arounds” on cyber security-related issues.⁴¹¹ NIPC published assessments, advisories, and alerts, including “CyberNotes,” which provided security professionals “with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.”⁴¹² Many cybersecurity experts also have pointed out that the alert system duplicates efforts of several private sector entities.⁴¹³

More recently, DHS announced the creation of a Cyber Interagency Incident Management Group to bring together officials from law enforcement, national security, and defense agencies for voluntary periodic meetings at a staff level for planning responses to major cybersecurity incidents. These agencies, however, gathered together before the Department and the NCSD existed under Richard Clarke’s direction to assess viruses and other computer incidents as they happened. Recreating the programs that existed two years ago simply is not enough if we are to protect our vital networks and infrastructures. More should be done to “facilitate interactions and collaborations” among the federal agencies tasked with cybersecurity responsibilities, as required by the Homeland Security Presidential Directive-7 (HSPD-7) issued in December 2003.

If DHS is to implement a successful cybersecurity agenda, it should fully engage the private sector. It has made some efforts to do so, including its participation in the National Cybersecurity Summit organized by several IT associations and entities last December. Despite these efforts, more should be done and DHS should fully consult with relevant private sector entities in developing comprehensive cybersecurity. For example, several ISACs were not consulted when DHS developed the cyberthreat e-mail service, even though it stated that it “will integrate very closely” with existing entities such as the ISACs. In response, Suzanne Gorman, chair of the financial services sector’s ISAC and head of the ISAC Council, stated “we talk about partnerships, but it would have been really nice if they had a conversation with us ahead of making this announcement.”⁴¹⁴ As a result, many of the private sector leaders responsible for sharing information about particular critical infrastructure sectors are not sure what new capabilities the alert system will offer, what is expected of them, or how DHS intends to integrate existing networks and private sector efforts into its plans.⁴¹⁵

Philip Reiting, Senior Security Strategist for Microsoft, testified to the House Select Committee on Homeland Security on July 15, 2003 that “without a multidisciplinary effort by both

⁴¹¹ U.S. Department of Homeland Security, “U.S. Department of Homeland Security Improves America's Cyber Security Preparedness--Unveils National Cyber Alert System,” press release, January 28, 2004, http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0337.xml.

⁴¹² National Infrastructure Protection Center, <http://www.nipc.gov/cybernotes/cybernotes.htm>.

⁴¹³ Michael Mimoso, “Where's the value in DHS' new alert system?” *Searchsecurity.com*, February 2, 2004, http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci947369,00.html.

⁴¹⁴ Dan Verton, “New DHS Cyber Alert System Under Fire,” *Computerworld*, February 6, 2004, <http://www.computerworld.com/securitytopics/security/story/0,10801,89550,00.html>.

⁴¹⁵ *Ibid.*

government and industry, we will not succeed” in protecting our cyber networks.⁴¹⁶ The Administration should improve its efforts to build a private-public partnership for securing cyberspace.

If a crisis were to occur, our nation would need structures and processes in place for real-time coordination among both the private and public sector. The United States does not have these structures in place, and private sector owners and operators of major critical infrastructures are not adequately engaged in efforts that will require numerous entities –within and outside the government – to respond.

SECURITY RECOMMENDATION

The challenges of protecting our critical networks and critical infrastructures require a new paradigm of government and industry leadership for addressing crises as they emerge. The Administration should take several actions if we are to avoid a cyber “9-11.”

First, the NCSD Director should have more authority and should report directly to Secretary Ridge or, alternatively, to the President to ensure that we are moving forward on the country’s cybersecurity efforts. Second, the Administration should move more rapidly to implement the National Strategy on Cyberspace. Finally, the Administration should create a National Crisis Coordination Center that could house within a single physical facility critical infrastructure representatives from the private sector and federal, state and local government agencies. This center would bring all the relevant parties together in the event of a cyber “9-11.”

SECURITY GAP: Government Networks Are Insecure.

Despite the growing threat of cyber attacks, government computer networks remain unprotected. In 1998, Presidential Decision Directive 63 required the federal government to reduce its exposure to threats and serve as a model on how to protect infrastructures. Five years later, this mandate remains unmet. Every year, the House Government Reform Committee’s Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census grades federal agencies on their cybersecurity practices in a “Computer Security Report Card.” In December 2003, eight of the agencies surveyed received a failing grade on the security of their computer network systems.⁴¹⁷ The grades were based on information contained in the agencies’ Federal Information Security Management Act (FISMA) reports to the Office of Management and Budget for fiscal year 2003.

Agencies receiving failing grades included DHS, Justice, Energy, and State – agencies that play critical roles in the protection of our homeland. Indeed, DHS, which houses the NCSD and is responsible for leading our nation’s cybersecurity efforts, received the worst score of any agency – 34 out of 100.

⁴¹⁶ U.S. House, Select Committee on Homeland Security, Subcommittee on Cybersecurity, Science, Research & Development, *Industry Speaks* Hearing, July 15, 2003.

⁴¹⁷ U.S. House, Committee on Government Reform, *2003 Federal Computer Security Report Card*, <http://reform.house.gov/TIPRC/Hearings/EventSingle.aspx?EventID=652> .

In FISMA, Congress provided federal agencies a framework for securing our computer network systems. Despite this framework, the government's computer networks largely remain insecure. One reason for this is that the government, overall, is not yet requiring vendors to deliver safe systems "out of the box" and ensuring that patches are delivered automatically.⁴¹⁸ Agencies demanding more secure products from vendors will help create more secure software and hardware.⁴¹⁹ When government agencies begin to require their vendors to comply with basic security needs, software and hardware producers will have a market incentive to produce more secure products.

In December 2003, DHS attempted to address the failure of the government to secure its computers by creating the Chief Information Security Officers Forum (CISO Forum) to "share information about programs that are successful and ones that are challenged and need assistance." Under FISMA, each agency must designate a "senior agency information security officer" to coordinate the agency's required security obligations. The Forum would bring these individuals together periodically and on a volunteer basis to share their experiences with cybersecurity within their respective agencies. While the creation of the Forum is commendable, it simply is not enough. The government lacks a single individual who serves as the U.S. government's Chief Security Officer (CSO) to ensure that the various agency CISOs are taking actions and improving the government's cybersecurity.

As long as critical government networks remain unprotected, our homeland security is at risk.

SECURITY RECOMMENDATION

The government should use its procurement power to demand secure products from vendors. Specifically, all government agencies should be required to follow the lead of the Department of Energy, which recently entered into a contract with Oracle requiring the company to deliver its database software preconfigured with the highest level security settings.⁴²⁰ In addition, the government should strengthen FISMA's security requirements for each agency by using a set of comprehensive collaborative benchmarks for procuring products that are "secure out of the box."

In addition, more and more companies are recognizing the need for company-wide CSOs as part of their leadership. According to the Gartner research firm, fifty percent of Global 2000 companies will have a CSO in place to handle information security by next year.⁴²¹ The Administration should create a Federal CSO within the Office of Electronic Government and Information Technology at the Office of Management and Budget who would be accountable and responsible for protecting government computers and developing solid programs throughout the

(Continued on following page)

⁴¹⁸ U.S. House, Select Committee on Homeland Security, Subcommittee on Cybersecurity, Science, Research & Development, *Cybersecurity – Growing Risk from Growing Vulnerability* hearing, June 25, 2003.

⁴¹⁹ Dan Verton, "Some See Hope Beyond Low Government Cybersecurity Grades," *Computerworld*, December 11, 2003, <http://www.computerworld.com/securitytopics/security/story/0,10801,88088,00.html?from=imuheads>.

⁴²⁰ Brian Krebs, "Energy Dept. Takes Lead in Security Experiment," *Washington Post*, September 23, 2003, <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A53958-2003Sep23¬Found=true>.

⁴²¹ Joel Strauch, "Spelling out the Chief Security Officer," *Talent Economy Magazine*, October 2003, <http://www.talenteconomymag.com/include/article2.php?articleID=280>.

government, as well as ensuring that the various federal agencies are complying with FISMA. This official would also determine which benchmarks are appropriate for agencies to use and oversee efforts to assist agencies in procuring products with greater security.

SECURITY GAP: “Cyber First-Responders” Lack Training and Education.

System administrators at companies across the globe are the first protectors and responders of the cybersecurity realm. Unfortunately, the private sector and government have found it difficult to find qualified workers for information security positions.⁴²² The challenge of providing specialized training for both technology professionals and home computer users extends to all levels of higher education and is especially relevant for those who provide supplementary training for those already in the workforce.⁴²³

According to the CERT Coordination Center, more than 95 percent of all known computer intrusions can be traced to known vulnerabilities and configuration errors. While “patches” are regularly made available by software and hardware vendors as vulnerabilities are discovered, many system administrators do not regularly apply patches unless there is a crisis or if a “fix” is deemed critical. The Blaster worm this past summer serves as a good example of this problem. Although Microsoft made available a patch to fix the flaw underlying the worm in July 2003, many users failed to install it on their computers, leaving them vulnerable. By August 2003, someone had created the Blaster worm to take advantage of the flaw. Within days of the worm being released, it had infected almost half a million computers.⁴²⁴ A trained and educated technical workforce is critical to alleviating this quick spreading of viruses and worms.

SECURITY RECOMMENDATION

In furtherance of the development of a culture of security in which all citizens are active contributors, the Administration should earmark funds for developing programs and regional laboratories at universities, colleges, and community colleges to educate information technology professionals about cybersecurity. These academic institutions are the ones that serve their regional workforces and can quickly develop relevant programs and curricula based on their ties with local businesses.⁴²⁵ For example, the student bodies of community colleges include first-generation college students, and workers seeking further education or training for new careers. As such, these institutions are also in the best position to develop a culture of security within their communities to ensure that all citizens are part of the plan to defend our homeland.

⁴²² National Science Foundation and American Association of Community Colleges, *Cybersecurity Education: The Role of Community Colleges in Protecting Information*, June 2002, http://www.aacc.nche.edu/Content/NavigationMenu/ResourceCenter/Projects_Partnerships/OtherInitiatives/Cybersecurity/Cyberreport.pdf.

⁴²³ Ibid.

⁴²⁴ Michelle Delio, “Blaster Worm Still Making Mayhem,” www.wired.com, August 30, 2003.

⁴²⁵ National Science Foundation and American Association of Community Colleges, *Cybersecurity Education: The Role of Community Colleges in Protecting Information*, June 2002, http://www.aacc.nche.edu/Content/NavigationMenu/ResourceCenter/Projects_Partnerships/OtherInitiatives/Cybersecurity/Cyberreport.pdf.

SECURITY GAP: Individual Users are Being Left Behind As Weak Links In the Battle To Secure Our Computer Networks.

While there have been some efforts, including DHS' creation of cyber bulletins for consumers, to educate home users about cybersecurity, much more needs to be done if we are to secure the weakest links in our computer networks. Since any computer can be used as a point of attack, if individual users do not secure their home systems properly and take an active role in cybersecurity defense, our nation's computers as a whole are vulnerable.⁴²⁶ Of particular concern is the possibility that thousands of home users' computers have been taken over without their owners' knowledge and will be used to launch "distributed denial of service attacks" (DDoS attacks) against critical computer networks.⁴²⁷ A DDoS attack occurs when an individual gains control over other people's computers, often through computer viruses, and then uses those computers to send a flood of requests to a particular computer network until it becomes overwhelmed and stops functioning.

The infected computers are often called "zombies," and there are estimates that at any given time thousands of individual users' computers are zombies. The most well-known DDoS attack, orchestrated by a fifteen-year old Canadian calling himself "MafiaBoy," occurred in 2000 and caused more than a billion dollars in damages by shutting down several major Internet sites for a week.⁴²⁸ It is well-documented that a terrorist organization could use DDoS attacks to compromise key technology systems – such as emergency-response 911 systems or communications systems of first responders – to amplify the consequences of a physical attack.⁴²⁹

In addition, the failure of individuals to implement security on new technologies such as broadband and wireless networks is leaving networks insecure. The term "broadband" refers to Internet access that is high-speed and constantly connected to the Internet and includes cable and Digital Subscriber Line (DSL) service. Unfortunately, if users using broadband do not use firewalls and antiviral programs they are at risk, especially since these services often are "always on."

Home users are also installing wireless networks at a staggering pace. The number of U.S. households with wireless networks is believed to have doubled from 3.1 million in 2002 to over six million last year.⁴³⁰ A number of these networks are unprotected and vulnerable to hackers. The remote nature of wireless networks makes them vulnerable to denial of service attacks. For example, a terrorist could block an entire radio communication channel by transmitting "junk" on certain frequencies, thereby tying up that channel. Bad actors can also "piggyback" on legitimate business and home wireless networks, illegally using those networks to anonymously commit crimes or acts of terror. In many cities, individuals are engaging in "warchalking," where they look for open computer networks and make chalk marks on sidewalks or building walls or post the information on websites so that other computer users can easily find open networks.

⁴²⁶ Cynthia Webb, "Security is in the Hand of the Users," *Washington Post*, August 13, 2003, <http://www.washingtonpost.com/wp-dyn/articles/A53577-2003Aug13.html>

⁴²⁷ Dennis Fisher, "Thwarting the Zombies," *e-week*, March 31, 2003, <http://www.eweek.com/article2/0,3959,985389,00.asp>.

⁴²⁸ "Mafiaboy Sentenced to 8 Months," *Wired News*, September 13, 2001, <http://www.wired.com/news/business/0,1367,46791,00.html>.

⁴²⁹ National Research Council of the National Academies, *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities*, (Washington DC, 2003).

⁴³⁰ Jonathan Krim, "WiFi Is Open, Free and Vulnerable to Hackers," *Washington Post*, July 27, 2003, A01.

SECURITY RECOMMENDATION

We should make sure that our citizens are not the “weak links” in today’s interconnected and networked environment. If computer networks and systems are to be adequately protected, we should “create cybersecurity awareness and education programs and partnerships with consumers, businesses, governments, academia, and international communities,” as Tatiana Gau of America Online testified during a Congressional hearing.⁴³¹ The government should work more closely with the private sector in developing awareness among our citizenry regarding the necessity of all Americans to protect their part of cyberspace. Specifically, the government and the private sector should establish a framework specifying the actions and best practices that government, Internet service providers, software and hardware vendors, and others should utilize to ensure that individual users are not left behind.

SECURITY GAP: Research and Development Efforts Lag.

There is a need for research and development focusing on preventing, responding, detecting, mitigating, and recovering from cyber attacks. “It is critical to maintain a long-term view and invest in research toward systems and operational techniques that yield networks capable of surviving attacks while protecting sensitive data,” testified Richard Perthia, the Director of the Carnegie Mellon CERT Center & Software Engineering Institute during a hearing before the House Select Committee on Homeland Security.⁴³²

According to the Institute for Information Infrastructure Protection, a consortium of twenty-three academic and not-for-profit research organizations focused on cybersecurity, additional research is needed in several areas including enterprise security management, response and recovery efforts, identification mechanisms, forensics, analysis of security properties and vulnerabilities, trust and authentication, wireless, metrics, legal, policy, and economic issues.⁴³³ Research and development in these areas will help better understand the weaknesses of our networks and systems and how to build stronger networks.

In November 2002, Congress took the important step of passing H.R. 3394, the Cyber Security Research and Development Act, which earmarked federal funds for cybersecurity research and development.⁴³⁴ The Act authorized \$903 million over five years to the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST) to ensure that the U.S. is better prepared to prevent and combat terrorist attacks on private and government computers. Unfortunately, the Administration continues to request fewer funds than those authorized by the Act. For Fiscal Year 2005, the President’s budget only requested \$76 million for the NSF and \$18.5 million for NIST. These totals are well below the \$128.25 million and \$61.4 million authorized for NSF and NIST, respectively, in the Act.

⁴³¹ U.S. House, Select Committee on Homeland Security, Subcommittee on Cybersecurity, Science, Research & Development, *Industry Speaks* hearing, July 15, 2003.

⁴³² U.S. House, Select Committee on Homeland Security, Subcommittee on Cybersecurity, Science, Research & Development, *Cybersecurity – Growing Risk from Growing Vulnerability* hearing, June 25, 2003.

⁴³³ The Institute for Information Infrastructure Protection, *Cybersecurity Research And Development Agenda*, January 2003, http://www.thei3p.org/documents/2003_Cyber_Security_RD_Agenda.pdf.

⁴³⁴ U.S. House, Committee on Science, *Summary of H.R. 3394*, <http://www.house.gov/science/hot/homeland/cybersum.htm>.

In May 2003, the DHS Science & Technology Directorate at DHS of Homeland Security announced it was creating a “Cyber Security Research & Development Center” to work with NSF and NIST on cybersecurity research and development.⁴³⁵ In early December, DHS announced that the Science & Technology Directorate planned to hire a program manager to help create the cybersecurity expert center.⁴³⁶ It currently has only a cybersecurity Research & Development director and a contractor working on cybersecurity research issues. Despite the Center and personnel announcements, it is unclear how much the Science & Technology Directorate will be able to accomplish with regards to cybersecurity as it has designated less than two percent of its budget specifically for cybersecurity research and development.⁴³⁷ For Fiscal Year 2005, the President’s budget has only requested \$18 million for cybersecurity research and development, a zero increase from the amount appropriated in Fiscal Year 2004 for cybersecurity research in the Science & Technology Directorate. If our country is to have a robust homeland security agenda relating to cybersecurity, the Administration should dedicate more resources to this effort.

SECURITY RECOMMENDATION

The Administration should provide adequate support and resources to the agencies tasked with the government’s cybersecurity research and development efforts, as well as provide funding to academia to develop cybersecurity programs and technologies that can be shared among government, universities, and the private sector. Research and development efforts should focus on all aspects of cybersecurity – prevention, detection, and response. To that effect, the Administration and Congress should fund the NSF and NIST at the Fiscal Year 2005 levels specified by Congress in the Cyber Security Research and Development Act.

⁴³⁵ U.S. Department of Homeland Security, *Testimony of Dr. Charles McQueary, Under Secretary, Science and Technology Directorate Before the Committee on Science, U.S. House of Representatives*, May 14, 2003.

⁴³⁶ Ted Leventhal and Greta Wodele, “Homeland Security science division will also tackle cybersecurity,” *govexec.com*, December 4, 2003, <http://www.govexec.com/dailyfed/1203/120403tdpm2.htm>

⁴³⁷ U.S. House, Committee on Science, *Hearing Charter: Cybersecurity Research and Development*, May 14, 2003.

Protecting the Food Supply

A biological attack against the nation's agricultural sector could result in a major public health crisis along with substantial economic and social disruption. The United States is currently unprepared for such acts of "agro-terrorism." Although a recent Presidential Directive establishes general guidelines for a national policy to defend against an agro-terrorism attack, it lacks specificity and falls short on implementation timeframes. The Administration should now move aggressively to develop a detailed national preparedness and response plan with meaningful action-oriented strategies and timeframes. Moreover, the Administration should strengthen inspection programs at food processing facilities and along our borders, as well as bolster the nation's disease surveillance capabilities.

Agricultural terrorism has received relatively little attention compared to other terrorist tactics, but the threat of these attacks by rogue factions is very real. Hundreds of pages of U.S. agricultural documents, translated into Arabic, were among the volumes of information left behind in al Qaeda caves after U.S. troop raids. A significant part of the group's training manual was reportedly devoted to the destruction of crops, livestock and food processing operations.⁴³⁸

Terrorists have already seen the ease of reaching a large volume of people through food contamination, both intentionally and unintentionally. In 1984, a cult group poisoned salad bars at Oregon restaurants with Salmonella bacteria, and 750 people fell ill.⁴³⁹ In January 2003, the Centers for Disease Control and Prevention reported that 92 persons became ill after consuming beef from a Michigan supermarket that was contaminated with nicotine.⁴⁴⁰

Apart from the catastrophic loss of human life, a successful bio-assault on agriculture could significantly undermine the national economy and carry social consequences. The food industry comprises 13 percent of our GDP⁴⁴¹ and provides jobs to one in eight Americans.⁴⁴² Deliberate contamination of crops and/or livestock would result in direct financial losses to all participants in agriculture and food production. For example, the recent discovery of a single case of mad cow disease (which is not considered a disease likely to be used for an agro-terrorism attack) in the U.S. seriously damaged international trade in American beef. The 2001 outbreak of foot and mouth disease in the United Kingdom, caused by a highly contagious and easily introduced virus, cost that country more than \$10 billion in economic losses.⁴⁴³ Apart from immediate revenue losses, producers may lose future market shares if distributors, wholesalers, and retailers choose alternative suppliers.

⁴³⁸ Katherine McIntire Peters, "Officials Fear Terrorist Attack on U.S. Food Supply," *Govexec.com*, June 10, 2003, <http://www.govexec.com/news/index.cfm?mode=report&articleid=25825>.

⁴³⁹ U.S. General Accounting Office (GAO), *Bioterrorism: A Threat to Agriculture and the Food Supply*, GAO-04-259T, (Washington, D.C: GPO, November 19, 2003), 4.

⁴⁴⁰ Ibid.

⁴⁴¹ Ibid, 1.

⁴⁴² Peter Chalk, *Hitting America's Soft Underbelly: The Potential Threat of Deliberate Biological Attacks Against the U.S. Agricultural and Food Industry*, RAND (2004), ix.

⁴⁴³ GAO, *Foot and Mouth Disease: To Protect U.S. Livestock, USDA Must Remain Vigilant and Resolve Outstanding Issues*, GAO-02-808, (Washington, D.C: GPO, July 26, 2002), 2.

The terror threat alone from even suspected contamination of the food supply could also cause economic disaster. In 1989, Chilean grapes were widely rumored to be laced with cyanide poison. Although no evidence was found, public fears cost the industry at least \$210 million in damages.⁴⁴⁴ Finally, panic and fear from an agricultural attack could lead to wide-spread social disruption and erosion of public confidence in the government's ability to protect the food supply.

Terrorists may find an attack on crops and livestock attractive because of its favorable cost-to-benefit payoff. A simulation of an intentional release of foot and mouth disease showed that a single truckload of contaminated hogs could spread disease to 25 states within five days before detection.⁴⁴⁵ Infecting plants or animals with deadly disease is also cheaper than infecting humans directly. Since no major U.S. city has more than a seven-day supply of food, consumers would feel the impact of a terror attack almost immediately.⁴⁴⁶ Moreover, the highly integrated nature of our food distribution system means numerous access points for terrorists as food travels from "farm-to-fork," moving thousands of miles and changing hands repeatedly.⁴⁴⁷

The Administration should address these threats to our agricultural sector and food supply.

SECURITY GAP: We Do Not Have A Comprehensive Agro-Terrorism Preparedness and Response Plan.

Over two and a half years after 9/11, the Administration has not developed a detailed national response strategy for preparing and defending the nation against agro-terrorism⁴⁴⁸ and numerous gaps remain in our ability to rapidly and effectively respond to these kinds of attacks.⁴⁴⁹ The current food safety system is still a confusing patchwork of different federal agencies, and layer of state programs, that continues to operate under disparate regulatory approaches in an uncoordinated fashion.⁴⁵⁰ One assessment has estimated that more than 200 government offices and programs could be involved in responding to an animal-borne disease outbreak.⁴⁵¹

The U.S. Department of Agriculture (USDA) and Federal Drug Administration (FDA) are principle among the myriad of federal agencies responsible for food safety and agro-terrorism. Now that a portion of USDA's Animal and Plant Health Inspection Service (APHIS) has been transferred to the Department of Homeland Security (DHS) under the Homeland Security Act of

⁴⁴⁴ Philip Hilts, "Don't Eat Grapes FDA Warns," *Washington Post*, March 14, 1989, sec. A1.

⁴⁴⁵ Daniel G. Dupont, "Food Fears: The Threat of Agricultural Terrorism Spurs Calls for More Vigilance," *Scientific American*, October 2003, 22.

⁴⁴⁶ Katherine McIntire Peters, "Officials Fear Terrorist Attack on U.S. Food Supply," *Govexec.com*, June 10, 2003, 2.

⁴⁴⁷ Congressional Research Service (CRS), *Food Safety Issues for the 108th Congress*, RL31853, by Donna U. Vogt, January 6, 2004, 2.

⁴⁴⁸ Corine Hegland, "Agriculture's Homeland Security Role Still in Seedling Stage, Observers Say," *National Journal.com*, January 9, 2004.

⁴⁴⁹ Rocco Casagrande, "Biological Terrorism Targeted at Agriculture: The Threat to U.S. National Security," *The Nonproliferation Review*, (Fall-Winter 2000), 1-14.

⁴⁵⁰ GAO, *Food Safety and Security: Fundamental Changes Needed to Ensure Safe Food*, GAO-02-47T, October 10, 2001, 3-10.

⁴⁵¹ Marilyn Werber Serafina, "Group Criticizes Public Health Leadership as Piecemeal, Haphazard," *Govexec.com*, January 14, 2004,

<http://www.govexec.com/news/index.cfm?mode=report2&articleid=27420>.

2002,⁴⁵² the federal regulatory maze has become more elaborate. This underscores the need for the Administration to develop a detailed national plan for agro-terrorism.

Sustained fragmentation hampers the effectiveness of federal food safety efforts and causes confusion about which federal entity should take the lead in the event of an agro-terrorism incident. Moreover, lack of coordination between federal agencies, their state counterparts, and private industry also continues to hinder our ability to respond effectively to an act of agro-terrorism. For years, a detailed national plan has been needed to identify how interrelated agricultural health and emergency management functions will be coordinated to ensure an orderly, immediate, and unified response to an agro-terror threat.

Over two years after 9/11, and with the nation still severely unprotected against the agro-terrorism threat, on January 30, 2004, the President issued Homeland Security Presidential Directive (HSPD)-9.⁴⁵³ This directive is a broad strategy which designates DHS as the lead agency for preventing and responding to acts of agro-terrorism and generally describes national goals and DHS' relationships with other federal agencies and state and local stakeholders.

Issuance of HSPD-9 was a much needed step. But the general nature of its guidance and lack of meaningful goals and timelines demonstrate that – consistent with the overall lack of action up to now – more effective and specific action is needed to fully prepare for possible acts of agro-terrorism.

SECURITY RECOMMENDATION

The Administration should move forward vigorously to develop a detailed national preparedness and response plan to combat agro-terrorism. The plan should include specific strategies and timeframes for vulnerability and response assessments and preparedness evaluations.

SECURITY GAP: Border and Facility Inspections Are Inadequate.

Defense against agricultural terrorism begins at the border, where the introduction of contaminants can be stopped. But inspection at U.S. borders remains weak, with the FDA inspecting only 2 percent of food imports under its jurisdiction.⁴⁵⁴

One specific concern is the absence of a plan for retaining sufficient agriculture specialist positions. DHS established these positions as part of its “One Face at the Border” initiative to retain experience in handling the complex laws, regulations, and science involved in agriculture inspections. These agricultural specialists transferred to DHS from USDA and are critical to maintaining the integrity of our food supply because they monitor the quality of produce imported from other countries. Under the initiative, DHS plans to offer agriculture specialists the opportunity to transfer to officer positions within the Bureau of Customs and Border Protection (CBP). According to interviews with a sample of agricultural specialists, an estimated 50 to 75 percent of them would choose to transfer-- and all cited “more career advancement opportunities”

⁴⁵² Homeland Security Act of 2002, §421 (P.L. 107-296).

⁴⁵³ Homeland Security Presidential Directive/HSPD-9,
<http://www.whitehouse.gov/news/releases/2004/02/20040203-2.html>.

⁴⁵⁴ Jason Peckenpau, “No Retraining for Agricultural Inspectors in Border Agency Plan,” *Govexec.com*, October 29, 2003.

as the reason they would transfer, if permitted.⁴⁵⁵ However, the Administration has not filled all of its current authorized agriculture specialist positions, let alone developed plans to fill the positions that could be vacated by those choosing to move to CBP Officer positions.⁴⁵⁶ Nor has it announced policies or timeframes governing the transfer of agriculture specialists to CBP. A massive transfer of specialists could potentially create a huge gap in our ability to inspect agriculture shipments coming across our borders.

Weaknesses also persist at the thousands of food processing and packing plants across the country. Basic security is poor, personnel are transient and rarely screened, and inaccurate or nonexistent record keeping make tracing contaminated food complicated and time-consuming. Moreover, inspectors are not always adequately trained or equipped with "state-of-the-art" detection technologies. Many small-scale processing plants do not keep accurate records of their distribution activities, which could make it difficult to trace a tainted food item back to its origin.⁴⁵⁷ Inspection resources are still insufficient to meet the increasing demand. The Gilmore Commission concluded that USDA's one percent increase in inspectors is probably not enough to cover the thousands of facilities required.⁴⁵⁸ Finally, while USDA and FDA have issued security guidelines for food processing facilities, these agencies lack the authority or the manpower to enforce their adoption.⁴⁵⁹

SECURITY RECOMMENDATION

USDA, FDA, and DHS should strengthen their inspection programs. Sufficient numbers of well-trained inspectors at agricultural and food processing facilities and at the nation's borders are essential. DHS should quickly develop contingency plans to address excessive transfers of agricultural inspectors to other units. The job of all inspectors will be made much easier with rapid, sensitive diagnostic techniques for pathogens—including the capability to recognize exotic animal and crop disease. The Administration should set priorities to foster research and development for such devices and techniques.

SECURITY GAP: Disease Surveillance Systems Are Weak.

- **Disease Detection and Reporting**

The ability to rapidly detect an agricultural disease outbreak is vital to minimizing harm to people, damage to the economy, and public concerns. Today, strong disease surveillance is

⁴⁵⁵ Information obtained in minority staff interviews during site visits to borders in 2003.

⁴⁵⁶ Based on figures provided to the Select Committee on Homeland Security, in correspondence dated October 4, 2003.

⁴⁵⁷ Dr. Peter Chalk, "The Bio-Terrorist Threat to Agricultural Livestock and Produce" testimony before the Senate Governmental Affairs Committee, November 19, 2003, 5.

⁴⁵⁸ Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Forging America's New Normalcy*, December 2003, 38, <http://www.rand.org/nsrd/terrpanel/>.

⁴⁵⁹ GAO, *Food-Processing Security: Voluntary Efforts Are Underway, but Federal Agencies Cannot Fully Assess Their Implementation*, GAO-03-342, (Washington, D.C.: GPO, February 124, 2003), 11-12.

hampered by farmers and ranchers unwilling to report disease for fear of economic losses and veterinarians unfamiliar with the signs of agro-terrorism.⁴⁶⁰

These limitations are aggravated by the limited capacity of our nation's animal and plant health laboratories. Too few of these facilities, crucial for accurate diagnoses, exist nationwide, and those that do have limited resources to receive, analyze, and identify many potential agro-terrorist agents.⁴⁶¹ For example, the National Animal Health Laboratory Network (NAHLN) remains in the pilot stage with laboratories in only 12 states.⁴⁶² Moreover, these laboratories cannot detect the full range of dangerous agents, lacking the capability to test for more than eight of the 37 foreign animal disease agents.⁴⁶³ As a result, an outbreak of certain diseases might go unnoticed for long periods. In other instances, widespread outbreaks would quickly overwhelm laboratories or lead to misjudgments about the true extent of disease. While the Administration has requested \$381 million in fiscal year 2005 to boost USDA spending to protect the nation against agro-terrorism, the majority of the request, \$178 million, is for a single project, the National Centers for Animal Health in Ames, Iowa. Only \$30 million is being requested for both plant and animal laboratory upgrades elsewhere. The American Association of Veterinary Laboratory Diagnosticians estimates that at least an additional \$85 million above current funding is required to expand the network.⁴⁶⁴ Communication and coordination between animal and plant health laboratories, clinicians, and producers is vital for determining and implementing appropriate and rapid response measures. Today, no such system exists for swift, integrated information exchange.⁴⁶⁵

SECURITY RECOMMENDATION

Financial risk management and insurance tools should be developed to compensate farmers and ranchers for the loss of livestock and crops caused by terrorism in order to encourage disease reporting. The federal government should partner with universities and the private sector to bolster the number of veterinarians and pathologists sufficiently trained to recognize exotic livestock and crop diseases.

The capacity of our nation's animal and plant health laboratories should be boosted. Sufficient funding should be provided to expand the NAHLN to include at least one laboratory in every

(Continued on following page)

⁴⁶⁰ Dr. Peter Chalk, "The Bio-Terrorist Threat to Agricultural Livestock and Produce" testimony before the Senate Governmental Affairs Committee, November 19, 2003.

⁴⁶¹ Committee on Biological Threats to Agricultural Plants and Animals, National Research Council, *Countering Agricultural Bioterrorism*, (Washington, D.C.: National Academy Press, 2003): 6, 107-109.

⁴⁶² American Association of Veterinary Laboratory Diagnosticians, *National Animal Health Laboratory Network*, May 30, 2003, <http://www.aavld.org/MainMenu2/NAHLN/NAHLN.pdf>.

⁴⁶³ (a) David Kinker, *National Animal Health Laboratory Network*, presented to the Secretary's Committee on Foreign Animal and Poultry Diseases, Riverdale, MD, February 4, 2004; (b) Committee on Foreign Animal Diseases of the United States Animal Health Association, *Foreign Animal Diseases*, 1998 Edition, (Richmond, VA: United States Animal Health Association, 1998), http://www.vet.uga.edu/vpp/gray_book/FAD/index.htm.

⁴⁶⁴ American Association of Veterinary Laboratory Diagnosticians, *National Animal Health Laboratory Network*, May 30, 2003, <http://www.aavld.org/MainMenu2/NAHLN/NAHLN.pdf>.

⁴⁶⁵ Committee on Biological Threats to Agricultural Plants and Animals, National Research Council, *Countering Agricultural Bioterrorism*, (Washington, D.C.: National Academy Press, 2003):6, 109-110.

state with the capability to conduct tests for the key agro-terror threat agents. The USDA should look to projects in public health, such as the Laboratory Response and the Health Alert Networks, as models for stronger laboratory communication and coordination.

- **Animal Disease Reporting**

Zoonotic diseases, caused by pathogens dangerous to humans but carried by animals, pose a particular risk to public health. The case of West Nile Virus, a mosquito born disease that can harm both people and animals is illustrative. In the summer of 1999, zoo and park workers noticed hundreds of dead crows and other birds in New York City parks. But public health officials were not aware of these events until after humans began to fall ill and die weeks later and initially dismissed that the two outbreaks could be linked.⁴⁶⁶ Without better integration of animal and public health surveillance systems, responses to these diseases will continue to be managed in a piecemeal and uncoordinated manner.⁴⁶⁷ However, few states have made efforts to strengthen links between their public health and animal surveillance systems.⁴⁶⁸ Meanwhile, as noted above, state veterinary and NAHLN member laboratories lack the capability to test for deadly CDC category A and B zoonotic agents such as Rift Valley fever and glanders.

For fiscal year 2005, the Administration announced a “Bio-Surveillance Initiative,” which would include new funding at USDA to improve animal surveillance and at DHS harvest and integrate this information with public health data. While a potentially useful step, it remains unclear whether a national, as opposed to regional architecture for this integration is optimal or whether DHS will have sufficient expertise to integrate animal and human health surveillance data and produce usable, actionable outcomes.

SECURITY RECOMMENDATION

Animal and human health tracking networks need to be integrated. Nationwide and regional web-based databases, constantly updated with new disease surveillance information, need to be established. Laboratories, infectious disease practitioners, and veterinarians should have access to these databases or a derivative alert system.

- **Food-Borne Illness Surveillance**

Surveillance is also the most important tool for detecting contamination of the food supply. A strong state and local public health infrastructure is critical to effective surveillance of foodborne illness, but the common reliance on passive surveillance, through which clinicians and laboratories report diseases only after they are confirmed, is slow, and can be ineffective because food-borne illnesses are often misdiagnosed or left undiagnosed. Active surveillance, which involves the direct soliciting of relevant health information from clinicians, is much more likely

⁴⁶⁶ GAO, *West Nile Virus Outbreak: Lesson for Public Health Preparedness*, GAO/HEHS-00-180, (Washington, D.C.: GPO, September 2000).

⁴⁶⁷ Trust for America’s Health, *Animal-Borne Epidemics Out of Control: Threatening the Nation’s Health*, August 2003, <http://healthyamericans.org/reports/files/Animalreport.pdf>.

⁴⁶⁸ Janet Heinrich, Director of Public Health Issues, General Accounting Office, testimony before the House Government Reform Committee, February 12, 2004.

to detect outbreaks rapidly. However, CDC's active surveillance program, FoodNet, covers less than 15% of the U.S. population.⁴⁶⁹ In addition, the microbial monitoring of food, done at processing plants and ports of entry, is fragmented and is not sufficiently integrated with surveillance to detect pathogens in the food system.⁴⁷⁰

SECURITY RECOMMENDATION

Active surveillance of food-borne illnesses, particularly those caused by pathogens likely to be intentionally introduced, should be expanded more quickly. Ultimately, a nationwide active surveillance program should be instituted by the CDC. Rapid, clinical diagnostic tools for major food supply threat agents should be developed and supplied to practitioners. Results from food sampling and inspection data need to be further integrated into food-borne surveillance systems. This effort, combined with targeted research, should improve Critical Control Point methods to detect food contamination.

⁴⁶⁹ GAO, *Food Safety: CDC is Working to Address Limitations in Several of Its Foodborne Illness Surveillance Systems*, GAO-01-973, September 2001.

⁴⁷⁰ Food and Nutrition Board, Institute of Medicine, *Scientific Criteria to Ensure Safe Food*, (Washington, D.C.: National Academies Press, 2003).

Protecting America with Information Technology

Effective use of information technology can improve the management and functions of the Department of Homeland Security (DHS) and strengthen counterterrorism programs and initiatives. Effectively managed, information technology can transform how we protect the homeland. Unfortunately, the Administration is not sufficiently taking advantage of information technology for homeland security needs, DHS information technology management is not nearly as effective as it needs to be, and DHS has not done enough to make our innovative private sector a full partner in defending the homeland.

One of the principal reasons for creating the Department of Homeland Security (DHS) was to fully integrate and coordinate disparate agencies that share the mission of protecting the homeland. The creation of DHS brought together 22 agencies and more than 180,000 employees into an organization that inherited as many as 8,000 information technology applications.⁴⁷¹ One hundred of these are considered major,⁴⁷² such as systems for threat identification and management, incident response, law enforcement, warning and alert communications, port of entry/exit management, and immigration. Effectively using information technology and building communications infrastructure is critical to fulfilling DHS's mission.⁴⁷³ According to The Brookings Institution, "information technology should represent perhaps the highest priority for homeland security efforts."⁴⁷⁴

Information technology can improve and strengthen counterterrorism programs and initiatives. For example, it can help speed the integration of terrorist watch lists, strengthen the security of our borders by improving our ability to spot fraudulent documents, and greatly improve information sharing and our ability to "connect the dots" among federal, state, and local governments, law enforcement, the intelligence community, and the private sector.

Using information technology effectively is also essential for DHS to operate as a unified organization. Smart investments in information technology to rationalize disparate or duplicative financial and personnel systems will boost DHS's effectiveness by giving its executives greater knowledge and control of DHS resources. For rank-and-file employees, delays or deficiencies in implementing common systems such as e-mail, directory services, payroll and benefits reduce worker productivity.

⁴⁷¹ DHS Chief Information Officer, Steven Cooper, speaking to the Commonwealth of Virginia IT Symposium 2003, as reported in Susan Menke, "At Virginia IT Summit, Cooper Says DHS Has Far to Go," *Government Computer News*, September 29, 2003.

⁴⁷² DHS Chief Information Officer, Steven Cooper, testimony before the House Government Reform Committee, "Hearing on Assessing Barriers to Information Sharing in the Department of Homeland Security," May 8, 2003.

⁴⁷³ Information technology integration is identified by the DHS Inspector General's Office as among the top management challenges facing DHS. See DHS Office of the Inspector General, *Major Management Challenges Facing the Department of Homeland Security*, (Washington, DC: DHS, March 18, 2003). See also, Information Technology Association of America (ITAA), Enterprise Solutions Division, "IT Top Ten War on Terrorism Issues," (Arlington, VA: ITAA, Winter 2003).

⁴⁷⁴ M. O'Hanlon, P. Orszag, I. Daalder, et al, *Protecting the American Homeland: One Year On*, (Washington, DC: The Brookings Institution, 2002, with a new preface, January, 2003), xix.

Finally, the information technology capabilities of our private sector are a unique and powerful competitive strength of the American economy. Technology skill and innovation have transformed America's economic productivity and warfighting capability over the past decade. The government must ensure that the private sector's technology expertise is a full partner in our efforts to protect the nation and fight terrorism.

SECURITY GAP: The Administration is Not Doing Enough to Take Advantage of Information Technology for Homeland Security Needs.

Secretary Ridge has stated that the Administration is using new technologies, a restructured homeland security organization, and streamlined processes to make the nation significantly more secure.⁴⁷⁵ To be sure, DHS has begun to make modest progress in some areas. For example, the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program has begun using biometrics to verify visa-holder identity at selected ports of entry. The Department's Chief Information Officer (CIO), Steven Cooper, has produced an initial draft of an Enterprise Architecture to serve as a strategic guidance document for its information-technology integration efforts.

Notwithstanding these steps, however, significant problems remain. According to the bipartisan Congressional Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001 (Joint Inquiry), while information technology remains one of this nation's greatest advantages, it has not been "fully [or] effectively applied in support of U.S. counterterrorism efforts."⁴⁷⁶ Persistent problems include "a reluctance [by the government and the intelligence community] to develop and implement new technical capabilities aggressively," a "reliance on outdated and insufficient technical systems," and "the absence of a central counterterrorism database."⁴⁷⁷

Specifically, according to DHS CIO Cooper:

Databases used for law enforcement, immigration, intelligence, public health surveillance, and emergency management have not been integrated in ways that allow us to comprehend each others' data or "connect the dots" to better prevent terrorist attacks and protect our people and infrastructure from terrorism. Technologies and cultures of agencies have [led] to 'islands of technologies' and barriers to information integration.⁴⁷⁸

According to The Brookings Institution, "the Administration still has no plan for quickly improving real-time information sharing... among the [broad] set of public and private actors

⁴⁷⁵ DHS Secretary, Tom Ridge, speech at the American Enterprise Institute, as reported in Dan Verton, "Ridge sees technology, agency restructuring bolstering homeland security: The head of Homeland Security says the nation is more secure than in 2001," *Computer World*, September 2, 2003.

⁴⁷⁶ House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, "Congressional Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001," (Joint Inquiry), December, 2002.

⁴⁷⁷ Ibid.

⁴⁷⁸ DHS Chief Information Officer, Steven Cooper, testimony before the House Government Reform Committee, "Hearing on Assessing Barriers to Information Sharing at the Department of Homeland Security," May 8, 2003.

who are vital to preventing to homeland attacks.”⁴⁷⁹ Similarly, the Markle Foundation Task Force on National Security in the Information Age (Markle Foundation) concluded that, “the government’s progress since September 11, 2001, toward building an adequate network has been slow and is not guided by an overall vision.”⁴⁸⁰ The Council on Foreign Relations Independent Task Force on America’s Response to Terrorism echoes these concerns and points out the critical need for the federal government to comprehensively implement information technology-system upgrades and systems integration in support of counterterrorism activities:

The federal government is ill equipped to perform data sharing and filtering tasks among federal agencies in Washington, much less mount an integrated counter-terror information technology campaign [with] state and local governments.... [It] will take years to specify and then implement, given the scale of these upgrades, the overhang of legacy computer systems, and the straightjacket of federal procurement procedures.⁴⁸¹

The Administration’s ability to create a unified terrorist watch list is the test case of its ability to deploy information technology to improve homeland security. There is strong bipartisan consensus on the urgent need to implement a unified terrorist watch list, and the problem was well recognized even before September 11. Watch list data from federal agencies is finite and reasonably well-defined (12 lists at nine agencies). The amount of data that needs to be integrated is significantly smaller than databases that are integrated on a regular basis in the private sector. The technology to succeed is readily available commercially.⁴⁸² Properly managed, technology-related aspects of integrating the watch lists should take no more than six to twelve months.⁴⁸³

Two-and-a-half years after September 11, however, the Administration has not succeeded in creating a comprehensive unified terrorist watch list supported by a robust integrated database that connects it in real time to all relevant stakeholders. While responsibility for integrating terrorist watch lists briefly resided at DHS, the task has now been assumed by the Terrorist Screening Center (TSC), which is part of the FBI.⁴⁸⁴ The failure to complete this basic and important information-sharing task casts serious doubt on the Administration’s ability to manage information technology projects generally.

⁴⁷⁹ M. O’Hanlon, P. Orszag, I. Daalder, et al, *Protecting the American Homeland: One Year On*, (Washington, DC: The Brookings Institution, 2002, with a new preface, January, 2003), xiv.

⁴⁸⁰ Markle Foundation Task Force on National Security in the Information Age, “Task Force Says Government Has Not Yet Taken Advantage of America’s Technology Expertise to Combat Terrorism,” press release, Markle Foundation, December 2, 2003.

⁴⁸¹ James J. Shinn and Jan M. Lodal, Council on Foreign Relations (CFR) Independent Task Force on America’s Response to Terrorism, *Red-Teaming the Data Gap*, (New York, NY: CFR, April, 2002).

⁴⁸² Ibid.

⁴⁸³ Markle Foundation Task Force on National Security in the Information Age, *Creating a Trusted Network for Homeland Security: Second Report of the Markle Foundation Task Force*, “Working Group Analyses, Working Group I: Networking of Federal Government Agencies with State and Local Government and Private Sector Entities” and “Appendix G,” (New York: Markle Foundation, December 2, 2003), 144. House Select Committee on Homeland Security interviews with various technology-industry experts and data integration experts.

⁴⁸⁴ GAO, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, GAO-03-322, (Washington: U.S. General Accounting Office, April 15, 2003). The White House, “New Terrorist Screening Center Established,” September 16, 2003. <http://www.whitehouse.gov/news/releases/2003/09/20030916-8.html>.

Within DHS itself, the Administration is facing problems in a number of critical areas. DHS is falling short on integrating basic systems that would improve the Department's daily operations and ensure that DHS is unified, well-run, and greater than the sum of its parts. In addition, border management systems suffer from data quality and availability problems, obsolescence, duplication, and a failure to exploit modern communications technologies.⁴⁸⁵

Despite its promises to "[merge] the personnel and pay systems of all DHS component agencies into a single system," and that, "the new system will be completed by the end of the [2003],"⁴⁸⁶ DHS has still not integrated and streamlined basic "back-office" systems within the Department, including important administrative functions like accounting, acquisition, procurement, grant management, asset management, and budgeting.⁴⁸⁷ As a result, the DHS may not even know how many employees it has at any given time. According to DHS CIO Cooper, "The Department keeps a running hand-tallied list of its staff, with the total varying from 190,000 to 225,000 depending on which of the 22 component agencies' 24 human resources systems are consulted."⁴⁸⁸ Furthermore, many Homeland Security employees continue to rely on their former agencies for important everyday functions like benefits⁴⁸⁹ and payroll. Outsourcing functions to other agencies can cost American taxpayers more, as other agencies charge DHS overhead and management fees for providing such services.⁴⁹⁰

The President's fiscal year 2005 budget includes \$102.5 million to support the creation of new human-resources systems and initiatives and also funds five new employees for the Business Transformation Office to assist in consolidating management processes, systems, and services. Nonetheless, DHS predicts that a central administrative system "may be years away," and acknowledges that DHS officials are just beginning to "set the initial requirements for the merger project."⁴⁹¹

Overall, the inability of DHS to effectively streamline its myriad systems slows and undermines the ability of the Department to "build employee and organizational identity and support" and "define the culture," factors highlighted by the GAO as critical to the Department's overall success.⁴⁹²

⁴⁸⁵ Data Management Improvement Act (DMIA) Task Force, *DMIA Task Force, Second Annual Report to Congress*, "Appendix: IT Summary Report," (Washington, DC: DHS, December 2003).

⁴⁸⁶ U.S. Department of Homeland Security, "DHS Announces New 'U.S. VISIT System' for Travelers as the Department Marks Its First 100 Days," press release, April 29, 2003.

⁴⁸⁷ Wilson Dizard, "DHS plan for Consolidating Back-Office Apps Emerges," *Government Computer News*, January 26, 2004.

⁴⁸⁸ Susan Menke, "At Virginia IT Summit, Cooper Says DHS has Far to Go," *Government Computer News*, September 29, 2003.

⁴⁸⁹ DHS Office of the Inspector General, memo in response to questions from the House Select Committee on Homeland Security, January 7, 2004. For example, ODP is obtaining administrative support from the DOJ-OJP; FPS is obtaining administrative support from the GSA; and the TSA obtains support services from the FAA. Also see, for example, memoranda of understanding between DHS and 1) the Department of Treasury, dated March 11, 2003; 2) the Department of Health and Human Services, dated February 28, 2003; and 3) the Department of Transportation, dated February 27, 2003.

⁴⁹⁰ Ibid.

⁴⁹¹ Catherine Santana, Director of the DHS Resource Management Transformation Office, from Wilson Dizard, "DHS plan for Consolidating Back-Office Apps Emerges," *Government Computer News*, January 26, 2004.

⁴⁹² GAO, *Major Management Challenges and Program Risks: Department of Homeland Security*, GAO-03-102, (Washington, DC: GAO, January, 2003), 8.

In the area of border protection, a team from the Los Alamos National Laboratory, as part of DHS's Data Management Improvement (DMIA) Task Force, recently analyzed all of the information-technology systems within the federal government involved in border control.⁴⁹³ Nearly all of these systems now reside within DHS.⁴⁹⁴ The DMIA concluded that border management systems suffer from the following problems:

- A wide range of data transfer connections exist that could seriously hamper the availability and timeliness of critical information to relevant systems;
- Most systems are obsolete because they are based on outdated technologies; modern communications technologies have not been fully exploited by any of the border management systems.
- Obsolete systems suffer from overlapping or duplicative operational capabilities; suffer from high maintenance costs; have extremely limited interoperability; and have little, if any, adaptability for emergencies, unexpected situations, or changing national priorities.

SECURITY RECOMMENDATION

When it comes to using information technology to improve homeland security, the Administration should have as its goal nothing less than "network-centric homeland security," akin to "network centric warfare" which proved so successful in the Iraq War.⁴⁹⁵ In practical terms, this means transforming DHS through the extensive use of up-to-date information technologies to more broadly and efficiently gather and disseminate information to field and headquarters personnel, allowing them to most effectively fulfill their homeland security mission.

Specifically, the Administration should follow the recommendation of the Markle Foundation to create, "a distributed information technology network to share terrorism-related information among federal, state, and local government agencies and the private sector."⁴⁹⁶ The

(Continued on following page)

⁴⁹³ DMIA Task Force, *DMIA Task Force, Second Annual Report to Congress*, "Appendix: IT Summary Report," (Washington, DC: DHS, December, 2003).

⁴⁹⁴ Beyond systems remaining at the Departments of State and Justice, nearly all of these systems are now within DHS, including IT systems from the Immigration and Naturalization Services, U.S. Customs, U.S. Coast Guard, Transportation Security Administration, and about 18 other federal agencies.

⁴⁹⁵ For general discussion of the effect of technology on American military and security strategy see Stan Crock, Paul Magnussen, and Lee Walczak, "The Doctrine of Digital War," *Business Week*, April 7, 2003. For a more technical discussion on network-centric warfare, see Office of the Assistant Secretary of Defense, Command and Control Research Program (CCRP), Department of Defense, http://www.dodccrp.org/NCW/ncw_chapter.htm.

⁴⁹⁶ Markle Foundation Task Force on National Security in the Information Age, "Task Force Says Government Has not Yet Taken Advantage of America's Technology Expertise to Combat Terrorism: Markle Task Force Addresses Actions Needed to Create Information Network to Enhance Security While Preserving Civil Liberties," press release, the Markle Foundation, December 2, 2003.

Administration should rapidly create, by the deadlines promised,⁴⁹⁷ a unified comprehensive terrorist watch list which is supported by a robust database that integrates all relevant information on terrorists from across the federal government. DHS should speed the integration of back-office systems, which will be critical to developing organizational unity and effective management within DHS. With respect to border systems, DHS should follow the recommendations of its own task force, the DMIA, to 1) streamline access to information; 2) determine the security benefits of integrating systems across agencies; 3) ensure the quality of data within database systems; 4) proactively avoid the obsolescence of technology; and 4) ensure that “new” systems are designed to easily accommodate change.⁴⁹⁸

SECURITY GAP: DHS Management of Information Technology is Weak.

While many of the information-technology problems facing DHS are to be expected given the size and complexity of the bureaucratic reorganization, the situation is made worse by 1) the organizational weakness of the Department’s Management Directorate; 2) instability and attrition within division-level information-technology management; and 3) the lack of a dedicated and robust information technology integration team.

Part of the Department’s less-than-effective information technology effort stems from an organizationally weak DHS CIO’s office, which resides within the Management Directorate. The DHS CIO currently has little or no direct authority over the divisional CIOs within the Department and the hundreds of disparate legacy systems and projects that they manage.⁴⁹⁹ The problem was described in recent testimony before the House Committee on Small Business. According to Patricia Driscoll, CEO of Frontline Defense Systems:

Recently, the Bureau of Citizenship and Immigration Services [BCIS] let out a [blank purchase agreement] worth \$500 million, [which] included anything [IT related] that BCIS intends to buy over the next few years. The way [it] is currently [written], it will exclude any small business.... [It] was put on the street after the CIO of Homeland Security, Steve Cooper, said that he did not want [it] to go out. Mr. Cooper and Undersecretary for Management, Janet Hale, said [it] did not fit the new departmental guidelines’ investment plan for IT or strategy for acquisitions... and would severely hurt the small business initiative put forward by the White House. What is the point of having a CIO if he is not given budget control over the Department’s IT? Giving him control of the IT money is the only way that that we are going to see the Department start behaving differently and the only way we are going to see some real initiatives on sharing

⁴⁹⁷ Terrorist Screening Center Director, Donna Bucela, staff briefing for the House Select Committee on Homeland Security, January 15, 2004. Deadlines described were for a test-phase database containing 60,000 records by the end of March, 2004 and a “final” database by June, 2004. Secretary Tom Ridge testified before the Senate Committee on Government Affairs on February 9, 2004 that names will be “aggregated into a single database” by the end of summer, 2004.

⁴⁹⁸ DMIA Task Force, *DMIA Task Force, Second Annual Report to Congress*, “Appendix: IT Summary Report,” (Washington, DC: DHS, December, 2003).

⁴⁹⁹ Wilson Dizard, “Homeland Security Forges a Systems Cadre: A Unified IT Operation Could Take Years to Develop,” *Government Computer News*, September 1, 2003: “The extent of [the CIO’s] control is far from complete...DHS has not completely centralized its procurement operations, and though major purchases are subject to approval by investment review boards, CIOs in component agencies wield significant power over personnel and investment decisions.”

resources.⁵⁰⁰

The Department's Chief Procurement Officer (CPO), also within the Management Directorate, suffers from similar weakness. The CPO does not have direct line authority over the procurement operations of any of the legacy procurement organizations inherited by DHS.⁵⁰¹ Lacking a single authority to make decisions and set policy for contracting activities across DHS, it will be difficult for the Department to improve operating efficiency and ensure that there is not duplication or redundancy among projects and spending across different DHS divisions.⁵⁰²

Furthermore, when DHS was created, there was no plan to provide procurement capabilities for the Information Analysis and Infrastructure Protection Directorate, the Science and Technology Directorate, or the Office of the Secretary. Instead, responsibility for contracting operations for those divisions now rests with the CPO's office. As of January, 2004, the CPO's office had only three procurement operations officers.⁵⁰³ By the CPO's own estimates, the CPO's office should likely have an operational staff of 90-100.⁵⁰⁴ Of that number, the CIO's office alone could require approximately 60 contracting operations staff.⁵⁰⁵

DHS procurement offices not under the CPO's direct control are also understaffed. For example, it is estimated that Transportation Security Administration's contracting staff is roughly 70 percent understaffed, Customs and Border Patrol is approximately 10-15 percent understaffed, and the Federal Emergency Management Agency is slightly understaffed.⁵⁰⁶ While the President's 2005 budget includes an additional \$2.5 million for contract support for DHS's Investment Review Board to help with technical review and program analysis, those resources are not sufficient to address serious resource shortfalls facing the CPO. The DHS may "simply [be] outnumbered by the personnel in its component parts"⁵⁰⁷

⁵⁰⁰ House Committee on Small Business, Subcommittee on Rural Enterprise, Agriculture and Technology, "Hearing on Challenges that Small Businesses Face Accessing Homeland Security Contracts," October 21, 2003.

⁵⁰¹ DHS Chief Procurement Officer, Greg Rothwell, staff briefing for the House Select Committee on Homeland Security, January 14, 2004. Legacy procurement organizations that do not report to the CPO include Federal Emergency Management Agency, the Coast Guard, the Secret Service, and the Border and Transportation Security directorate and its constituent offices, the Transportation Security Administration, Customs and Border Protection, Federal Law Enforcement Training Center, and Immigration and Customer Enforcement.

⁵⁰² GAO, *Major Management Challenges and Risks: Department of Homeland Security*, GAO-03-102, (Washington, DC: GAO, January, 2003), 17: "DHS will be faced with the challenge of integrating the procurement functions of many of its constituent programs and missions. Early attention to strong systems and controls for acquisitions and related business processes will be critical to ensuring success and maintaining integrity and accountability."

⁵⁰³ DHS Chief Procurement Officer, Greg Rothwell, staff briefing for the House Select Committee on Homeland Security, January 14, 2004.

⁵⁰⁴ Ibid.

⁵⁰⁵ Ibid.

⁵⁰⁶ Ibid.

⁵⁰⁷ Wilson Dizard, "Homeland Security Forges a Systems Cadre: A Unified IT Operation Could Take Years to Develop," *Government Computer News*, September 1, 2003: "According to a study by the transactional records Access Clearinghouse of Syracuse University, in March [2003] the immediate office of secretary Tom Ridge had a staff of only 33, out of the department's total complement of more than 160,000 employees.... Undersecretary for Management Janet Hale had a staff of only 113 to oversee DHS business functions, including Cooper's operations." The Administration's fiscal year 2005 budget requests \$17 million for additional DHS headquarters staff, yet, even if approved, such additional personnel will not be largely available until after 2004, and still may not be sufficient.

In addition to a weak CIO's office, other layers of the Department's information-technology management are unstable. According to the DHS Office of the Inspector General, turnover among divisional CIOs since the Department opened its doors has been 45 percent.⁵⁰⁸ It is critical that DHS have a "strong and stable implementation team" to manage DHS's integration.⁵⁰⁹

Compounding a weak CIO's office, a weak CPO's office, and unsettled division-level information-technology management, DHS efforts also suffer from the lack of a dedicated information-technology integration team. According to the GAO, it is important to "dedicate an implementation team to manage the transformation process"⁵¹⁰ and that such a team "have direct access and be accountable to top leadership."⁵¹¹ With strong executive backing from the most senior DHS leadership, such a team would be empowered to prioritize, manage, and implement information technology projects anywhere within DHS. A dedicated integration team would have no allegiance to any particular operating directorate. It would, therefore, be able to focus on results and on projects of high strategic value to the Department as a whole.

Without such an integration team, "organizational fragmentation, technological impediments, or ineffective collaboration [will] blunt the nation's collective efforts to prevent or minimize terrorist acts."⁵¹² Efforts to streamline or merge DHS systems are likely to be hampered by bureaucratic infighting as managers seek to preserve particular programs or systems in which they have invested or with which they have become accustomed.

DHS CIO Cooper acknowledges the problem:

Something [I] might have done differently at the start... was to keep the dedicated integration team [that had been formed] at the White House Office of Homeland Security... We dissolved it, but maybe keeping it in place longer would have been beneficial.⁵¹³

Instead of a dedicated integration team with clear authority to initiate and implement important projects, large or small, anywhere within the Department, DHS has a three-tiered investment-management board to review technology projects based largely on project cost.⁵¹⁴ This structure may not be optimally organized to address critical integration issues with the speed and attention they deserve because factors other than dollar size may be significantly more important when deciding which projects to pursue and with what level of urgency. Furthermore, only the top level board, which looks at information-technology projects with life-cycle costs above \$200 million, includes senior DHS leadership with *de-facto* department-wide authority. The two

⁵⁰⁸ DHS Office of the Inspector General, memo in response to questions from the House Select Committee on Homeland Security, January 7, 2004.

⁵⁰⁹ GAO, *Major Management Challenges and Risks: Department of Homeland Security*, GAO-03-102, (Washington, DC: GAO, January, 2003), 9.

⁵¹⁰ Ibid, 7.

⁵¹¹ Ibid, 9.

⁵¹² Ibid, 17.

⁵¹³ Susan Menke, "At Virginia IT Summit, Cooper Says DHS Has Far to Go," *Government Computer News*, September 29, 2003.

⁵¹⁴ The investment threshold levels for each of the boards is as follows: the Investment Review Board reviews capital reviews projects with contractor costs greater than \$50 million and IT projects with life-cycle costs greater than \$200 million; the Management Review Council reviews projects with capital costs between \$5-\$50 million and IT projects with the life cycle-costs of \$20-\$200 million; the Enterprise Architecture Board reviews projects with annual costs of \$1-\$5 million and life-cycle costs of \$5-\$20 million.

“lower” boards, which review projects smaller than \$200 million, are comprised of the CIO, other Management Directorate executives (the CPO and Chief Financial Officer) or their designees, and divisional representatives. In light of the organizational weakness of the CIO and the CPO, as previously discussed, these two other boards lack sufficient Department-wide authority to prioritize and rapidly implement information-technology projects that are important to the integration of DHS as a whole. As long as DHS lacks a properly structured, nimble, and empowered information-technology integration team, progress with information-technology integration will be unacceptably slow.

SECURITY RECOMMENDATION

The DHS should rapidly strengthen its management and procurement of information technology by strengthening the offices of the Department’s CIO and CPO. The Administration should create a specific budget line item and robust budget justification detail for all of DHS’s information-technology related spending; supporting detail on projects and programs should be organized by strategic mission, regardless of where within DHS the activities reside. To improve management accountability, improve transparency and facilitate oversight, DHS should establish clear performance goals for information technology projects, set forth clear milestones and timelines, and be in a position to provide regular progress updates on initiatives in relation to those milestones and timelines.⁵¹⁵ Finally, the Administration should follow the recommendation of the Council on Foreign Relations and create an information-technology integration “Red Team,” which includes leading private sector experts, to advise the Department on how to accelerate information technology projects and quickly plug critical technology integration gaps.

SECURITY GAP: The Administration is Not Taking Sufficient Advantage of Private-Sector Expertise.

While Secretary Ridge has acknowledged the critical importance of making contracting easier for the nation’s innovative technology vendors,⁵¹⁶ DHS has not yet done enough to make it easier for private sector technology companies to work with DHS. In testimony before the House Committee on Small Business, witnesses expressed frustration with the lack of a reliable and comprehensive one-stop online resource to identify existing contract opportunities. According to Benjamin Brink, President and CEO of Data Search Systems:

[One] of the best business practices which make sense is one-stop shopping. [DHS] says that they are working on that, but [I did] a web search [to find out] where I might do business with the DHS.... [T]he DHS website took me [to] eight or nine agencies [and]

⁵¹⁵ For the importance of timelines and milestones to DHS technology projects, see for example, GAO, *Aviation Security: Computer Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385, (Washington, DC: GAO, February 12, 2004). See also, GAO, *Major Management Challenges and Risks: Department of Homeland Security*, GAO-03-102, (Washington, DC: GAO, January, 2003), 7.

⁵¹⁶ DHS Secretary Ridge, “Protecting the Homeland: The President’s Proposal for Reorganizing Our Homeland Defense Infrastructure,” testimony before the Senate Committee on the Judiciary, June 26, 2002. According to Secretary Ridge, “The new Department should have flexible procurement policies to encourage innovation and rapid development and operation of critical technologies vital to securing the homeland.”

gave few links to regulations. I could not find anything about HSARPA [the Homeland Security Advanced Research Project Agency].... [The] website of [Representative Steven Buyer had] far better information on small businesses doing business with the DHS than the DHS did.⁵¹⁷

At the same hearing, Daniel Lane, CEO of the EMCOM Project stated that:

[H]ow we normally find out about the contracts is [to] hang out at the Capitol Hill Club.... I find out more stuff down there than I do ever attending any meeting.... Unfortunately I find out about [business opportunities with DHS] in a bar.... We are continuing to check the contracting websites on a day-to-day basis.⁵¹⁸

SECURITY RECOMMENDATION

The Administration should ensure the rapid creation of a robust, comprehensive, up-to-date, and easy-to-use one-stop resource (web, phone, fax, support) for companies wishing to do business with DHS. The system should serve as both a means of communication with the private sector and as a management tool that allows DHS executives to quickly determine the progress and status of important projects.

⁵¹⁷ House Committee on Small Business, Subcommittee on Rural Enterprise, Agriculture and Technology, "Hearing on Challenges that Small Businesses Face Accessing Homeland Security Contracts," October 21, 2003.

⁵¹⁸ Ibid.

PREPARING OUR COMMUNITIES

Preparing Our Nation's First Responders

One year after the formation of the Department of Homeland Security, and more than two years after September 11, America's first responders are still not properly equipped, trained, or staffed to protect our communities from a terrorist attack. In certain respects, we have not even taken the first steps towards reaching an acceptable level of preparedness, because there has been no systematic review of the true planning, equipment, training and personnel needs of America's first responders. While the Administration continues to propose multiple, disparate sources of funding for emergency responders, it has not defined the goals and objectives of this spending, nor has it identified the priority threats and vulnerabilities that limited homeland security funds should address. Most of our first responders still do not have interoperable communications equipment, and the Administration has not taken bold steps to resolve this critical deficiency. In the opinion of an independent task force chaired by former Senator Warren Rudman, "the United States remains dangerously ill-prepared to handle a catastrophic attack on American soil." The Select Committee on Homeland Security has crafted bipartisan legislation to determine the needs of all our communities and to create a single first responder grant program that will get the best equipment and training in the hands of the police, firefighters and emergency personnel who will be the first on the scene of an attack.

In the aftermath of September 11, 2001, there was a broad recognition among policymakers and lawmakers that the preparedness and response capabilities of our first responders – police, firefighters, emergency medical service, public health agencies and hospitals, public works agencies, and emergency management agencies – needed to be significantly strengthened to meet the threat of terrorism in the homeland. Overall, fire departments across the country have only enough radios to equip half the firefighters on a shift, and breathing apparatuses for only one third.⁵¹⁹ Police departments in cities nationwide do not have the protective gear to safely secure a site following an attack with weapons of mass destruction, and most cities do not have the necessary equipment to determine what kind of hazardous materials emergency responders may be facing.⁵²⁰ All terrorist incidents are local or at least will start that way. Effective preparedness, response, and recovery can only be achieved with the recognition that local responders are the first line of defense, and that these responders must have the resources to fulfill their critical roles in the fight against terrorism.⁵²¹

⁵¹⁹ Federal Emergency Management Agency, United States Fire Administration, *A Needs Assessment of the U.S. Fire Service, FA-240* (Washington: Federal Emergency Management Agency, December 2002), vi.

⁵²⁰ Council on Foreign Relations, *Report of an Independent Task Force Sponsored by the Council on Foreign Relations, Emergency Responders: Drastically Underfunded, Dangerously Unprepared* (New York: Council on Foreign Relations, June 2003), 1.

⁵²¹ Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Fourth Annual Report to the President and the Congress* (Arlington, VA: RAND, December 2002), 27-28.

SECURITY GAP: Preparedness Needs Have Not Been Defined.

All levels of government have recognized the critical need to bridge the “security gap” by providing additional funding for first responder planning, training, exercises, and equipment nationwide. In FY 2004, it is estimated that the Federal government will spend approximately \$5.4 billion⁵²² on these efforts, while State and local governments will spend between \$5.2 and \$15.2 billion.⁵²³ However, one year after the creation of the Department of Homeland Security (DHS), these funding levels are completely arbitrary because the Administration has yet to conduct a systematic review of the actual needs of the first responder community. While the Administration requests and Congress continues to provide funding for emergency responders, we have not defined the goals and objectives of this spending, nor have we identified the threats and vulnerabilities that will be mitigated by additional homeland security funds. Therefore, we do not know if the current funding levels are sufficient to close the “security gap” facing our communities, and we have no way to measure progress towards the goal of providing communities with the ability to respond to a catastrophic act of terrorism.

Numerous observers from across the political spectrum – including the DHS Office of the Inspector General – have repeated the critical need for such measures of progress:

“DHS program managers have yet to develop meaningful performance measures necessary to determine whether the grant programs have actually enhanced state and local capabilities to respond to terrorist attacks and natural disasters.”⁵²⁴

“This lack of broad but measurable objectives is unsustainable. It deprives policymakers of the information they need to make rational resource allocations, and renders program managers unable to measure genuine progress. It also suggests endlessly escalating program expenditures, since there is no logical end point to a process whose only goal is to improve from current standing.”⁵²⁵

⁵²² (a) “Fiscal Year 2004 Homeland Security Appropriations Act,” (P.L. 108-90), *United States Statutes at Large*, 117 Stat. 1137; (b) U.S. House, 108th Congress, 1st Session. *H.R. 2673, Fiscal Year 2004 Consolidated Appropriations Act*, ONLINE, GPO Access, Available: <http://www.congress.gov/omni2004/H25NO032.PDF> [January 7, 2004]; (c) Council on Foreign Relations, *Report of an Independent Task Force Sponsored by the Council on Foreign Relations, Emergency Responders: Drastically Underfunded, Dangerously Unprepared* (New York: Council on Foreign Relations, June 2003), 29-30.

⁵²³ Council on Foreign Relations, *Report of an Independent Task Force Sponsored by the Council on Foreign Relations, Emergency Responders: Drastically Underfunded, Dangerously Unprepared* (New York: Council on Foreign Relations, June 2003), 29-30.

⁵²⁴ U.S. Department of Homeland Security, Office of the Inspector General, *Major Management Challenges Facing the Department of Homeland Security*, ONLINE, December 31, 2003, Department of Homeland Security, <http://www.dhs.gov/interweb/assetlibrary/FY04managementchallenges.pdf> [February 10, 2004].

⁵²⁵ Richard A. Falkenrath, “The Problems of Preparedness: Challenges Facing the U.S. Domestic Preparedness Program,” *Executive Session on Domestic Preparedness Discussion Paper, ESDP-2000-05* (December 2000), 15, http://bcsia.ksg.harvard.edu/BCSIA_content/documents/The_Problems_of_Preparedness.pdf [February 18, 2004].

“... without a comprehensive approach to measuring how well we are doing with the resources being applied at any point in time, there will be very little prospect for answering the question ‘How well prepared are we?’”⁵²⁶

“But if the nation’s plan for enhancing security is to become a reality, the government will need to determine if, in fact, the tens of billions of dollars in fact produce greater security—and if all American citizens can count on at least a minimum level of security in their travel, homes, and places of business.”⁵²⁷

This situation persists because DHS has not defined national standards of preparedness – the essential capabilities to which every jurisdiction of a particular size should have or have immediate access. It is, therefore, not yet possible to determine precisely the gaps in each jurisdiction between how prepared it is now and how prepared it needs to be. Without such standards and guidelines, such as technical specifications for equipment and minimum training standards, both state and local governments and first responders lack sufficient information to determine their preparedness needs and priorities, as well as the true costs of their needs. National capability standards would make it possible to use funding efficiently to meet identified needs and measure preparedness levels on a local, state, regional, and national scale. Under the current DHS system, however, states are annually allocated an arbitrary amount of funds without any guidance as to how these funds should be further allocated to meet national preparedness goals.

In a July, 2003, hearing before the House Select Committee on Homeland Security, Massachusetts Governor Mitt Romney testified that in order to determine the degree of risk and the necessary levels of protection within his state, the DHS should provide guidelines, templates, and best practices from other states. These types of tools would allow him to answer questions such as, “What is the appropriate level? What is the level which is being practiced in other states? What is the best practice?”⁵²⁸

The GAO has recommended that, given the need for an integrated approach to homeland security, national performance goals and measures might best be developed in a collaborative way, involving all levels of government and the private sector.⁵²⁹ GAO further reported,

“The establishment of specific national goals and measures for homeland security initiatives, including preparedness, will not only go a long way towards assisting state and local entities in determining successes and areas where improvement is needed, but could also be used as goals and performance measures as a basis for assessing the effectiveness of federal programs. [...] Given the recent and proposed increases in homeland security funding, as well as the need for real and meaningful improvements in

⁵²⁶ Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Fourth Annual Report to the President and the Congress* (Arlington, VA: RAND, December 2002), 37.

⁵²⁷ Donald F. Kettl, “Promoting State and Local Government Performance for Homeland Security,” *The Century Foundation Homeland Security Project* (June 1, 2002), 1, http://www.homelandsec.org/Pub_category/pdf/state_local_gov_perform.pdf [February 18, 2004].

⁵²⁸ U.S. House, Select Committee on Homeland Security, *First Responders: How States, Localities, and the Federal Government are Working Together to Make America Safer* Hearing, July 17, 2003.

⁵²⁹ U.S. General Accounting Office, *Homeland Security: Effective Intergovernmental Coordination Is Key to Success*, GAO-02-1011T (Washington: U.S. General Accounting Office, August 2002), 13.

preparedness, establishing clear goals and performance measures is critical to ensuring both a successful and fiscally responsible effort.”⁵³⁰

The current first responder funding process, however, is irrational; neither DHS nor the grant recipients have a “preparedness baseline” to measure the nation’s progress towards enhanced preparedness for response to acts of terrorism. The annual distribution of funding for planning, equipment, training, and exercises from DHS’s first responder grant system is arbitrary and based on political and budgetary considerations, rather than a rational assessment of needs in light of the terrorist threats and critical infrastructure vulnerabilities facing our communities.

State allocations for the first fiscal year 2004 homeland security grants announced by the DHS Office for Domestic Preparedness (ODP) continue to reflect the lack of any true assessment of the threats and vulnerabilities facing our nation.⁵³¹ Under the current distribution formula, each state receives 0.75 percent of the total grants available in each fiscal year. The rest of the money is distributed based on population.⁵³² Based on this formula, states such as California, New York, Texas and Florida receive less than \$6 per capita, while low-population states such as Wyoming, North Dakota and Vermont receive more than five times as much per person.⁵³³ Federal homeland security spending of \$38 per capita in Wyoming and less than \$6 per capita in Texas and California certainly do not reflect the threats and vulnerabilities likely facing those states.

For fiscal year 2005, the President’s budget request for grants to our state and local first responders increases the level of discretionary grant funds that will be distributed to states and localities based on threats and vulnerabilities identified by DHS. At the same time, however, the fiscal year 2005 request represents close to an \$800 million – or 18 percent – decrease from the amounts appropriated by Congress in fiscal year 2004.⁵³⁴ Yet, DHS has not conducted any published studies or developed any metrics to confirm how much states and localities have improved their preparedness for acts of terrorism, and therefore can provide no rationale for the overall reduction in first responder grant funds.⁵³⁵

In a hearing before the House Select Committee on Homeland Security (Select Committee), Los Angeles County Police Captain Michael Grossman recommended the formation of a “first responder/emergency manager” task force to serve as a federal advisory group to ensure effective distribution of grant funds.⁵³⁶ In September 2003, Democratic members of the Select Committee introduced the PREPARE Act (H.R. 3158), which would require DHS to create an independent, expert state and local task force comprised of representatives from first responder communities as

⁵³⁰ Ibid, 15.

⁵³¹ U.S. Department of Homeland Security, *Remarks by Secretary of Homeland Security Tom Ridge Announcing FY04 ODP Grant Allocations*, ONLINE, November 3, 2003, Department of Homeland Security, Available: <http://www.dhs.gov/dhspublic/display?content=2174> [January 7, 2004].

⁵³² “USA Patriot Act of 2001.” (P.L. 107-56, § 1014(c)(3)), *United States Statutes at Large*, 115 Stat. 272.

⁵³³ Alice Lipowicz, “Cox Says Administration Unwilling to Change Formula for Homeland Security Grants,” *CQ Homeland Security*, November 3, 2003, <http://homeland.cq.com/hs/news.do> [February 18, 2004].

⁵³⁴ U.S. Department of Homeland Security, *Budget in Brief, Fiscal Year 2005*, (Washington: Department of Homeland Security, February 2004), 57.

⁵³⁵ Justin Rood, “CNA Snags \$7.4 Million Deal to Help DHS Assess State and Local Preparedness,” *CQ Homeland Security*, February 17, 2003, <http://homeland.cq.com/hs/news.do> [February 19, 2004].

⁵³⁶ U.S. House, Select Committee on Homeland Security, *First Responders: How States, Localities, and the Federal Government are Working Together to Make America Safer* Hearing, July 17, 2003.

well as other experts.⁵³⁷ This task force would develop standards and guidelines for states and localities to use to identify the essential terrorism prevention, preparedness, and response capabilities required by any generic community of a given population and geographic size, utilizing threat and vulnerability information to guide the determination of such capabilities. The Select Committee's Subcommittee on Emergency Preparedness and Response included the PREPARE Act's requirement for this task force, in addition to numerous other PREPARE Act provisions, in bipartisan first responder grant legislation that was unanimously approved on November 20, 2003.⁵³⁸

As stipulated in the bipartisan legislation, the task force would specify capability needs – including equipment, personnel, training, planning, and exercises – for firefighting, law enforcement, emergency medical services, public health systems, hospitals, and emergency management, that are flexible enough to be used for a wide range of threats and vulnerabilities. These capabilities can be developed and maintained within the community, as part of a regional agreement among communities, or at the state government level. In this fashion, annual grant funding from the DHS will be better budgeted and targeted to meet the needs assessed by the states and localities, allowing us to measure progress towards closing the “security gap.”

SECURITY RECOMMENDATION

Congress should promptly enact this bipartisan legislation and the President should sign it into law. Annual allocations of grant funding no longer will be based on irrational formulas; state and local capability needs – and the grant funds provided by DHS – will vary based on the real threats and vulnerabilities faced by each state and local community, leading to a more rational allocation of available resources.

Passage of the Select Committee's bipartisan legislation would address the frequently-voiced need for additional investments to build state and local preparedness capabilities. Independent analyses have noted that homeland security spending over the next five fiscal years (FY 2004 – FY 2008) would need to be tripled to meet the preparedness needs of our first responders.⁵³⁹ Mayors in the nation's largest cities continue to advocate higher levels of funding for training and prevention activities associated with increased threats, in addition to requesting an expansion of the allowable uses of current funds so that these mayors can address their top security priorities.⁵⁴⁰

(Continued on following page)

⁵³⁷ U.S. House, 108th Congress, 1st Session. *H.R. 3158, Preparing America to Respond Effectively Act of 2003*, ONLINE, GPO Access, Available: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h3158ih.txt.pdf [January 28, 2004].

⁵³⁸ U.S. House, Select Committee on Homeland Security, *Faster and Smarter Funding for First Responders Act of 2003* Markup, November 20, 2003.

⁵³⁹ Council on Foreign Relations, *Report of an Independent Task Force Sponsored by the Council on Foreign Relations, Emergency Responders: Drastically Underfunded, Dangerously Unprepared* (New York: Council on Foreign Relations, June 2003), 2.

⁵⁴⁰ (a) U.S. House, Select Committee on Homeland Security, *H.R. 3266: Faster and Smarter Funding for First Responders Act of 2003* Hearing, October 16, 2003; (b) U.S. Conference of Mayors, “90 Percent of Cities Left Empty-Handed Without Funds from Largest Federal Homeland Security Program: Cities First To Respond, Last In Line For Funding Reveals First-Ever, 50-State Analysis,” September 17, 2003, http://www.usmayors.org/uscm/news/press_releases/documents/homelandfunding_091703.pdf [February 18, 2004].

By defining—for the first time—the preparedness needs of our communities, this legislation would provide an appropriate, sustained level of investment in preparedness for our first responders.

SECURITY GAP: Administration's Preparedness Goal Requires Legislation.

On December 17, 2003, in apparent recognition of the serious shortcomings in first responder preparedness grant programs, the White House issued Homeland Security Presidential Directive Number 8 (HSPD-8) on National Preparedness.⁵⁴¹ Similar to the PREPARE Act and the Select Committee's legislation, this directive requires DHS to define a national preparedness goal, to provide grant funding in support of achieving this preparedness goal based on a true assessment of the risks faced by grant applicants, and to define standards for first responder equipment.

SECURITY RECOMMENDATION

To truly advance the goals set forth in HSPD-8, the Administration should support prompt enactment of the Select Committee's legislation. Enactment of the Select Committee's legislation would revise the grant systems to meet the Administration's goal of allocating funds based on risk.

SECURITY GAP: Existing Grant Programs are Not Effective.

Not only are the current DHS terrorism preparedness grant programs unrelated to a valid assessment of overall needs and required capabilities, these programs are also confusing, duplicative, inefficient, and mired in bureaucracy. In November 2002, GAO reported to Congress on the development of counter-terrorism programs for state and local governments that were similar and potentially duplicative.⁵⁴² Later, in April 2003, GAO testified that they had identified at least 16 different grant programs that were being used by the nation's first responders to address the nation's homeland security needs, including both terrorism-specific grant programs as well as "all-hazards" grant programs. GAO stated that multiple fragmented grant programs such as these can create a confusing and administratively burdensome process for state and local officials seeking to use federal resources for their pressing homeland security needs.⁵⁴³

Mayors in the nation's largest cities have repeatedly voiced their frustrations with the homeland security grant process. Mayor James A. Garner testified before the Select Committee's Subcommittee on Emergency Preparedness and Response that an October 2003 survey conducted

⁵⁴¹ The White House, *Homeland Security Presidential Directive/HSPD-8*, ONLINE, December 17, 2003. The White House, <http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html> [January 7, 2004].

⁵⁴² U.S. General Accounting Office, *Combating Terrorism: Funding Data Reported to Congress Should Be Improved*, GAO-03-170 (Washington: U.S. General Accounting Office, November 26, 2002).

⁵⁴³ U.S. General Accounting Office, *Federal Assistance: Grant System Continues to be Highly Fragmented*, GAO-03-718T (Washington: U.S. General Accounting Office, April 29, 2003), 8.

by the United States Conference of Mayors (USCM) found that more than half of the 168 cities surveyed had either not been consulted or had no opportunity to influence state decision-making about how to use and distribute fiscal year 2003 homeland security grant funds. The survey also found that 80 to 90 percent of cities had not received funds from the largest DHS homeland security grant program in fiscal year 2003, ODP's state homeland security grant program.⁵⁴⁴ A January 2004 follow-up survey by the USCM revealed that 76 percent of cities still had not received any fiscal year 2003 funds from the state homeland security grant program.⁵⁴⁵

The fragmented delivery of federal assistance complicates coordination and integration of services and planning at state and local levels. Homeland security is a complex mission requiring the coordinated participation of many federal, state, and local government entities as well as the private sector. Preparing the nation to address the new threats from terrorism requires partnerships across many disparate actors at many levels in our intergovernmental system. For example, local governments have started to assess how to restructure relationships among contiguous local entities in order to take advantage of economies of scale, promote resource sharing, and improve coordination on a regional basis. The complex web of federal grants described by GAO suggests that by allocating federal aid to different players at the state and local level, federal grant programs may continue to reinforce state and local fragmentation.⁵⁴⁶

Currently, there are multiple preparedness funding streams, each with different rules, formulas, and customers. In DHS press releases, these programs often are cited jointly and combined into overall "First Responder" funding to demonstrate responsiveness to the needs of the emergency preparedness community.⁵⁴⁷ However, as noted by GAO, the overlap and fragmentation among these programs have fostered inefficiencies and numerous concerns among first responders. State and local officials have repeatedly voiced frustration and confusion about the burdensome and inconsistent application processes among programs.⁵⁴⁸

SECURITY RECOMMENDATION

As originally proposed in the PREPARE Act, the Select Committee's bipartisan legislation would combine multiple DHS first responder preparedness grants into a single "First Responder Grant Program." This new program would distribute grants to states and localities to achieve preparedness capability needs based on the current threats and vulnerabilities they face. The grant program will be administered by one office within DHS, in order to establish a single

(Continued on following page)

⁵⁴⁴ U.S. House, Select Committee on Homeland Security, *H.R. 3266: Faster and Smarter Funding for First Responders Act of 2003* Hearing, 16 October 2003.

⁵⁴⁵ U.S. Conference of Mayors, "Mayors Release New Homeland Security Survey at 72nd Winter Meeting of the U.S. Conference of Mayors: Second Mayors' Report to the Nation Shows Money Still Log-Jammed at State Level," January 22, 2004, http://usmayors.org/72ndWinterMeeting/homelandreportrelease_012204.pdf [February 18, 2004].

⁵⁴⁶ U.S. General Accounting Office, *Federal Assistance: Grant System Continues to be Highly Fragmented*, GAO-03-718T (Washington: U.S. General Accounting Office, April 29, 2003), 13.

⁵⁴⁷ U.S. Department of Homeland Security, "Helping Our Nation's First Responders," ONLINE. June 5, 2003, Department of Homeland Security, <http://www.dhs.gov/dhspublic/display?content=910> [January 7, 2004].

⁵⁴⁸ U.S. General Accounting Office, *Federal Assistance: Grant System Continues to be Highly Fragmented*, GAO-03-718T (Washington: U.S. General Accounting Office, April 29, 2003), 14.

organizational entity that is responsible for maintaining all information on the grants and regular communication with all grant recipients.

The legislation also includes specific provisions to ensure that local governments receive federal homeland security grant funds no later than 45 days after the state government receives such funds, including allowing communities to request direct payment of grant funds from DHS if the state fails to pass through grant money in the required timeframe. Finally, to encourage cooperation across city, county, and state boundaries, and to speed the distribution and use of grant funds, the legislation allows intra- and inter-state regions to apply directly to DHS for homeland security grant funds. This regional concept was first developed in legislation introduced by Representative Christopher Cox (R – CA), Chairman of the House Select Committee on Homeland Security (H.R. 3266).

SECURITY GAP: First Responders Still Cannot Communicate.

Perhaps the most critical need of our emergency response community is a significant enhancement of their ability to communicate during times of crisis. Today, new and evolving technologies can bring news and entertainment to the farthest reaches of the world. At the same time, many law enforcement officers, firefighters, and emergency medical service personnel working in the same jurisdiction cannot communicate with one another at the scene of an emergency. The inability of our public safety officials to readily communicate with one another threatens the public's safety and often results in unnecessary loss of lives and property.⁵⁴⁹

However, DHS and other federal agencies are not moving quickly and efficiently to address the interoperable communications needs of first responders. There are at least six federal departments and a number of interagency and independent organizations that are involved in developing standards for communication systems and equipment.⁵⁵⁰ This situation makes it difficult for states and local entities to know what to buy, and increases the possibility of purchasing incompatible equipment. Further, despite the fact that the Homeland Security Act of 2002 mandated that no less than four organizations within DHS – including the Office of the Secretary – address and administer the implementation of interoperable communications systems,⁵⁵¹ only one state and local grant program to address this critical issue has been implemented in the year since DHS was established.

In fiscal year 2003, DHS, in coordination with the Department of Justice Office of Community Oriented Policing Services (COPS), awarded a total of \$146.5 million in grants for local jurisdictions across the nation to conduct demonstration projects that will explore uses of equipment and technologies to increase communications interoperability. However, in a hearing before the House Select Committee on Homeland Security, Michael Brown, DHS Undersecretary for Emergency Preparedness and Response, indicated that it will take approximately six months

⁵⁴⁹ National Task Force on Interoperability, *Why Can't We Talk? Working Together To Bridge the Communications Gap to Save Lives: A Guide for Public Officials* (Washington: National Task Force on Interoperability, February 2003), 2.

⁵⁵⁰ Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Fifth Annual Report to the President and Congress*, (Arlington, VA: RAND, December 15, 2003), 26.

⁵⁵¹ "Homeland Security Act of 2002," (P.L. 107-296, § 102(c)(2), 232(b)(7), 430(c)(2), and 502(7)), *United States Statutes at Large*, 116 Stat. 2143, 2159, 2191, and 2212.

to more than a year to complete these projects, to be followed by a DHS study and the development of national standards.⁵⁵²

In addition, the Administration's fiscal year 2004 budget request did not include any specific funds for State and local governments to enhance or implement interoperable communications systems. The only fiscal year 2004 funds for this purpose – \$85 million – were provided by Congress under the Department of Justice COPS program, representing a \$61.5 million, or 42 percent, reduction from fiscal year 2003 program levels. For fiscal year 2005, the Administration's budget requests no funds for interoperable communications grants for state and local governments. Given the fact that DHS has requested no funding for enhancing state and local interoperable communications in fiscal year 2005, first responders continue to be concerned that the Federal efforts in this area are fragmented and uncoordinated.⁵⁵³

At present, the only continuing DHS effort to address interoperable communications resides in the Wireless Public Safety Interoperable Communications Program (SAFECOM) office within the Science and Technology Directorate. Established by OMB, SAFECOM serves as the umbrella program within the federal government to assist federal, state, and local public safety agencies improve response through more effective and efficient interoperable wireless communications. DHS serves as the "managing partner" for SAFECOM, with eight other federal agencies contributing resources to the effort. For fiscal year 2005, DHS and the other federal agencies are requesting a total of \$22.1 million for SAFECOM to create a process for developing interoperability standards, to coordinate federal grant guidance, to provide training and technical assistance, and to perform research and development on emerging interoperable communications technologies.⁵⁵⁴

However, SAFECOM officials recently have noted that no standard, guidance, or national strategy exists on interoperability. Justice Department officials informed GAO that they are working with SAFECOM to develop a statement of requirements for interoperability that should be ready for release by May 1, 2004.⁵⁵⁵ In other words, more than two years and eight months after the loss of New York City first responders due to the non-interoperability of their communications systems, the Administration intends to issue a statement describing the need for interoperability standards.

On February 23, 2004, Secretary Ridge announced that improving interoperable communications and equipment was the department's second highest priority.⁵⁵⁶ However, DHS's proposed solution of providing "technical specifications" for short-term, baseline communications is nothing new. Many state and local government officials have already identified and deployed

⁵⁵² U.S. House, Select Committee on Homeland Security, *Response to Terrorism: How is DHS Improving Our Capabilities* Hearing, June 19, 2003.

⁵⁵³ Alice Lipowicz, "Police Get \$85 Million to Pursue Interoperability," *CQ Homeland Security*, December 3, 2003, <http://homeland.cq.com/hs/news.do> [February 18, 2004].

⁵⁵⁴ U.S. Department of Homeland Security, *Department of Homeland Security Science and Technology Fiscal Year 2005 Congressional Budget Justification* (Washington: Department of Homeland Security, February 2, 2004), 30-31.

⁵⁵⁵ U.S. General Accounting Office, *Homeland Security: Challenges in Achieving Interoperable Communications for First Responders*, GAO-04-231T (Washington: U.S. General Accounting Office, November 6, 2003), 8.

⁵⁵⁶ U.S. Department of Homeland Security, "Fact Sheet: The U.S. Department of Homeland Security: Preserving Our Freedoms, Protecting Our Nation," ONLINE, February 23, 2004, Department of Homeland Security, <http://www.dhs.gov/dhspublic/display?content=3208> [February 24, 2004].

such systems, but lack the resources to further enhance interoperable communications within their jurisdictions.

SECURITY RECOMMENDATION

While the Administration continues to conduct studies and wait for the development of nationwide standards before providing significant funding for interoperable communications systems, there are a number of interim solutions that can be implemented in the short term to improve communications interoperability for our first responders. Various technologies are available to “patch” or connect different radio frequencies. The simplest form of patching is installing a radio that can access another system in the dispatch center and making an audio connection with wiring. A more technologically advanced system is also available that can connect each attached radio through a switching system.⁵⁵⁷ Further, a number of federal government contractors already have developed and deployed mobile emergency operations centers that include multiple communications capabilities to facilitate interoperability during emergency response. The Administration should immediately implement these interim solutions by providing dedicated, annual funding for enhancements to state and local interoperable communications systems in order to address this critical need of our first responders.

The Administration should also address the disjointed federal approach to interoperability by clearly assigning principal responsibility for communications interoperability standards to the DHS Project SAFECOM Office, and by providing this office with the annual funding it requires to develop and rapidly implement standards for interoperable communications equipment.

The Select Committee’s bipartisan legislation, H.R. 3266, addresses each of these issues. The Administration should support and sign into law this legislation in order to provide our first responders with rapid access to and regular, annual funding for technologies that facilitate interoperable communications; to move more quickly to develop standards for interoperable communications systems; and to coordinate all federal programs in support of interoperable communications within DHS.

SECURITY GAP: Civil Preparedness Must Be Improved.

In addition to preparing our emergency response community, it is imperative that citizens of the United States be informed of terrorist incidents, and understand what actions to take in the face of a terrorist attack or threatened terrorist attack. As the authors of the Progressive Policy Institute Homeland Security Report Card state, “this preparedness is key to reducing panic and saving lives.”⁵⁵⁸ Efforts to address civil preparedness and public notification of terrorist incidents by DHS and the Administration through the Ready.gov website are lacking in detail and are sometimes contradictory. Few individual Americans – at home, at work, and in schools – understand what they should do or whom to turn to for guidance in the event of a terrorist attack.

⁵⁵⁷ National Task Force on Interoperability, *Why Can't We Talk? Working Together To Bridge the Communications Gap to Save Lives: A Guide for Public Officials* (Washington: National Task Force on Interoperability, February 2003), 30-31.

⁵⁵⁸ Progressive Policy Institute, *America at Risk: A Homeland Security Report Card* (Washington: Progressive Policy Institute, July 2003), 13.

And there is no national plan for how to communicate with individuals during a terrorist incident to advise them what to do.⁵⁵⁹

SECURITY RECOMMENDATION

The Administration should enhance its civil preparedness efforts by developing a coordinated and comprehensive campaign to inform the public of specific actions they should take in the event of a chemical, biological, radiological, or other weapon of mass destruction incident. The Administration should also support legislative initiatives to implement nationwide notification networks to ensure that all citizens have the information they need, and the actions they should take, following a terrorist attack

⁵⁵⁹ U.S. House, 108th Congress, 1st Session. *H.R. 2250, To amend the Homeland Security Act of 2002 to direct the Secretary of Homeland Security to develop and implement the READICall emergency alert system*, GPO Access, Available: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h2250ih.txt.pdf [February 19, 2004].

PRESERVING OUR VALUES

Reinforcing Security, Privacy, and Civil Liberties

The United States has long been a beacon for democracy around the world. Strengthening our homeland security ensures that our way of life and the rights bestowed by the U.S. Constitution remain intact. As the Administration develops and employs new technologies and gathers information from the private sector for our homeland security efforts, it must ensure that our society's constitutional guarantees relating to privacy, due process, and civil liberties are protected.

The protection of our nation's civil liberties and privacy is fundamental to the American way of life. Our homeland security efforts are, after all, designed to preserve the "unalienable rights that are essential to the strength and security of our nation: life, liberty, and the pursuit of happiness."⁵⁶⁰ As the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (the Gilmore Commission) found in 2003, "security" and "civil liberties" are mutually reinforcing parts of the effort to strengthen our homeland.⁵⁶¹

The development of homeland security initiatives requires our government to protect fundamental constitutional rights and to strive to minimize unnecessary impositions on the freedoms and privileges enjoyed in the United States. The Gilmore Commission found that "[g]overnments must look ahead at the unintended consequences of policies in the quiet of the day instead of the crisis of the moment."⁵⁶² As our government develops post 9/11 homeland security initiatives in areas such as immigration, intelligence collection, law enforcement, and the use of new technologies it should thoughtfully and carefully review their impact on our fundamental freedoms.

Our first obligation is to pay close attention to the law enforcement and other authorities the government acquires in the name of fighting terrorism. Congress passed the USA PATRIOT Act in response to the attacks of September 11. The Act increased the ability of law enforcement and intelligence agencies to more effectively share information about terrorists and their activities, broadened federal authority to track and intercept communications for both law enforcement and foreign intelligence gathering purposes, provided for the detainment and deportment of alien terrorists, and added resources to fight terrorism financing. While some parts of the USA PATRIOT Act have provided important counterterrorism tools, concerns have been expressed that other sections of the legislation extend overly intrusive authorities to the government. Congress wisely provided that certain wiretapping and foreign intelligence provisions would expire after four years so that the efficacy of these provisions and their impact on personal liberty could be carefully assessed. Our country should have this important debate, as the Gilmore Commission put it, "in the quiet of the day," before moving to extend the expiration date of these provisions.

⁵⁶⁰ Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, also known as the Gilmore Commission, *Forging America's New Normalcy: Securing Our Homeland, Protecting Our Liberty*, December 2003, http://www.rand.org/nsrd/terrpanel/volume_v/volume_v_report_only.pdf.

⁵⁶¹ Ibid.

⁵⁶² Ibid.

Our country needs to have a national discussion as well on how innovative technologies and information sharing and collection systems should be used to protect the homeland. Technology gives federal agencies the capability to access homeland security information in a cohesive manner, regardless of whether that information is held in databases and networks at different agencies, thereby increasing the likelihood that we can identify potential terrorists. In doing so, however, the government should ensure that information is accurate, remains confidential, and that access is limited to only appropriate personnel so as to protect civil liberties and privacy. Given the sensitivity of information gathered about individuals, it is also imperative that this data be protected during its creation, transmission, and storage.⁵⁶³

Likewise, if the government uses information that is held by the private sector, it should do so within a system of rules and guidelines that protect civil liberties. In today's technology-dependent, transaction-friendly society, Americans produce millions of records of their daily activities – ranging from credit card purchases to government registration and accounting systems to logs of personal time spent on the Internet and in entertainment venues. Unchecked access to such information by the government and other entities without sufficient cause could violate many of our constitutional rights.

In addition, voluntary disclosure of personal customer information gathered by private sector entities to government agencies for data-mining projects - without notification to those customers - continues to raise concerns. For example, in September 2003 JetBlue admitted that it had given five million passenger itineraries, possibly through the assistance of the Transportation Security Agency (TSA), to a defense contractor as part of a study seeking ways to identify high risk customers.⁵⁶⁴ More recently, Northwest Airlines admitted that it handed over three months of passenger records to the National Aeronautics and Space Administration in 2001 for a data mining project. These disclosures were done without notification to customers, almost all of whom are presumably law-abiding individuals with no connections to terrorists. Consequently, the Federal Trade Commission and the Departments of Defense and Homeland Security are investigating the JetBlue disclosure, while two class action lawsuits have been filed against Northwest claiming that the airline illegally shared the private information.⁵⁶⁵

In the past year, several homeland security initiatives have been derailed or postponed because the Administration has failed to adequately evaluate the programs' effects on privacy and civil liberties. The Terrorism (first known as Total) Information Awareness (TIA) project, an initiative within the Defense Advanced Research Project Agency's Information Awareness Office, exemplifies the problem of developing programs without fully considering their impact on individual privacy. The program was designed to analyze as much information as possible on individuals and use computers and human analysis to detect potential terrorist activity. It planned to search existing databases containing information such as financial records, medical records, communication records, and travel records to find matches for particular patterns.⁵⁶⁶ Concerns

⁵⁶³ Markle Foundation's Task Force on National Security in the Information Age, *Protecting America's Freedom in the Information Age*, October 2002, and *Creating a Trusted Network for Homeland Security*, December 2003.

⁵⁶⁴ Thomas Claburn, "Northwest CEO Urges Airline Execs To Talk Privacy," *Information Week*, January 22, 2004, <http://www.informationweek.com/story/showArticle.jhtml?articleID=17500687>.

⁵⁶⁵ Ryan Singel, "Army Quietly Opens JetBlue Probe," *Wired*, November 26, 2003, <http://www.wired.com/news/privacy/0,1848.61374.00.html>.

⁵⁶⁶ Defense Advanced Research Projects Agency, *Report to Congress regarding the Terrorism Information Awareness Program In Response to Consolidated Appropriations Resolution, 2003, Public Law 108-7, Division M, § 111(b)*, May 20, 2003, http://www.darpa.mil/body/tia/tia_report_page.htm

regarding civil liberties and privacy led to TIA's cancellation, with Congress eliminating the Information Awareness Office responsible for creating the program.

Concerns are also raised by the Computer Assisted Passenger Prescreening System (CAPPS) II, which uses databases to check airline passengers' backgrounds and scores them on their potential to be risks. Various civil liberties and privacy issues have been identified with CAPPS II, including the lack of safeguards in place to protect passengers wrongly identified as terrorists, as well as questions regarding whether adequate security protections are in place to keep hackers and other criminals from accessing the personal information of passengers. As a result, Congress mandated that the program not be deployed until the General Accounting Office (GAO) completed a privacy and civil liberties assessment of the program.⁵⁶⁷ The GAO report, released on February 12, was inconclusive on TSA's privacy efforts. The report found that "[u]ntil TSA completes its privacy plans and the program is further developed," it could not be determined if the agency had identified all of the privacy risks and necessary mitigation efforts.⁵⁶⁸

Some of these projects might have been successfully implemented if civil liberties and privacy had been given great attention during their development. Benjamin Franklin once said "they that would give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." Our government should strive to be better in its implementation of new programs to protect our homeland, as Americans deserve both their liberty and safety.

SECURITY GAP: There is No Framework in the Government for Evaluating the Security and Privacy of New Technologies.

In a 2003 report, the Markle Foundation's Task Force on National Security in the Information Age found that the government lacked a "systematic effort to consider the privacy implications of the proposed programs or to develop an overall policy framework that would govern the deployment of new technologies."⁵⁶⁹ To protect civil liberties, a framework should be in place that the government can use to secure new technologies and develop privacy-protecting processes. To effectively combat terrorism and protect privacy, a framework establishing clear policies and guidelines is needed to "identify the types of databases involved, define the purposes of the data review, and clarify the authorization for collecting and disseminating whatever is found."⁵⁷⁰ Such a framework could assist the government's homeland security efforts, allowing it to use technology to better manage and sort the large amount of data it gathers.

A framework also can help us ensure that databases used across the government operate within federal privacy laws and do not offend our constitutional values. Protecting our homeland and protecting our citizen's privacy should not be a "balancing act" where one is sacrificed for the benefit of the other. Rather, homeland security and privacy should reinforce one another through safeguards that build oversight and restraints on the misuse of power into our security initiatives.

⁵⁶⁷ Judi Hasson, "Congress Demands Study of CAPPS II," *fcw.com*, September 26, 2003, <http://www.fcw.com/fcw/articles/2003/0922/web-capps-09-26-03.asp>.

⁵⁶⁸ U.S. General Accounting Office, *Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, February 13, 2004, Available at <http://www.gao.gov>.

⁵⁶⁹ Markle Foundation Task Force on National Security in the Information Age, *Creating a Trusted Network for Homeland Security*, December 2003, 14.

⁵⁷⁰ Markle Foundation Task Force on National Security in the Information Age, *Protecting America's Freedom in the Information Age*, October 2002, 36.

Technology has advanced significantly, with the advent of biometrics, supercomputing, interconnected global networks, the Internet, and other new technologies. Indeed, a bipartisan proposal by former government officials from the Clinton and Reagan administrations found that to properly protect our citizen's privacy the federal government should take into account "the revolutionary changes in recent years in communication, surveillance and database technology, and the implications of those changes for individual privacy and personal liberties."⁵⁷¹

Unfortunately, the federal government has not conducted a comprehensive assessment of the use of new technologies and privacy in 30 years. The original Privacy Act of 1974 established the "U.S. Privacy Protection Study Commission" to evaluate the statute and issue a report on how to improve privacy protections. The Commission issued its report "Personal Privacy in an Information Society" in 1977 and ceased its operations. Since that time, there has not been a comprehensive national government-wide effort to evaluate the privacy implications of new technologies.

SECURITY RECOMMENDATION

To secure our nation, we should create an environment that protects sensitive information and individual civil rights.⁵⁷² By defending civil liberties we can strengthen our homeland defense and our country. In order to ensure that a comprehensive privacy and homeland security evaluation is completed, the Administration should create a new Commission on Privacy, Freedom, and Homeland Security.⁵⁷³ This Commission would be charged with evaluating how we can organize our homeland security efforts in a manner that protects our nation and civil liberties and privacy in accordance with the fundamental values of our country. The Commission would create a comprehensive framework on the use of new technologies for homeland security that can provide guidance to the federal government on evaluating the purpose behind new technologies, the treatment of information gathered on individuals, and the access and distribution of information that might be gathered. The Commission would establish safeguards and protections for government access to and the use of individuals' personal information from commercial databases and lists. In particular, the Commission would devise mechanisms by which individuals could challenge and correct mistakes in databases that are utilized by the federal government. The Commission would also assess federal and state privacy statutes, evaluating how those laws are helping or hindering the protection of our homeland.

SECURITY GAP: Private Databases are Being Shared With the Government Without Customer Notification.

In January, the Department of Homeland Security (DHS) announced that it will require all airline carriers and reservation companies to submit personal information collected about their customers to the government as part of the CAPPS II program. Currently, airlines are not legally required to

⁵⁷¹ Peter Swire and Jeffrey Eisenach, "Ensuring privacy's post-attack survival," *Zdnet.com*, September 11, 2002, <http://zdnet.com.com/2100-1107-957464.html>.

⁵⁷² Markle Task Force on National Security in the Information Age, *Creating a Trusted Network for Homeland Security*, December 2003, 44.

⁵⁷³ Peter Swire and Jeffrey Eisenach, "Ensuring privacy's post-attack survival," *Zdnet.com*, September 11, 2002, <http://zdnet.com.com/2100-1107-957464.html>.

notify customers that they may submit passengers' personal information to the government for screening and analysis.

SECURITY RECOMMENDATION

Private sector entities that share with the federal government personal information of their customers held in commercial databases should be required to notify their customers of that fact, so long as that disclosure does not affect ongoing civil or criminal investigations. For example, airline carriers and reservation companies should be required, at the time of ticketing, to let customers know that their information will be turned over to the federal government as part of programs such as CAPPs II. In addition, procedures should be in place to allow customers to correct erroneous information about themselves in databases that might be shared with the federal government.

SECURITY GAP: The Government Lacks Essential Privacy Office.

The Administration is not doing enough to evaluate and protect civil liberties and the Constitution in today's environment of new technologies and new security concerns, as demonstrated by the controversies surrounding TIA, the Jet Blue disclosure, and CAPPs II. This is partly due to the fact that the Administration has neither a single office within the federal government responsible for evaluating privacy issues within the government nor designated officers within every agency to review privacy issues.

In 1998, President Clinton required every agency to "designate a senior official within the agency to assume primary responsibility for privacy policy."⁵⁷⁴ The next year, he created a "chief counselor for privacy" position for the federal government within the Office of Management and Budget (OMB) to advise on privacy issues. The counselor reviewed proposals before they went public and when there were privacy problems fixed them before the proposals were implemented.⁵⁷⁵ The privacy counselor position was eliminated, however, at the beginning of the current Administration. Many of the privacy leaders within the federal agencies left the government and were not replaced.⁵⁷⁶ No senior official within the White House or OMB has been designated to evaluate privacy in new technologies throughout the federal government.

Recognizing the need to have someone responsible for privacy relating to homeland security programs, Congress required DHS to create a "privacy office," tasking it with the following:

- Ensuring that DHS complies with the Privacy Act of 1974;
- Adequately considering privacy when DHS collects, uses, and discloses personal information; and

⁵⁷⁴ William J. Clinton, *Memorandum for the Heads of Executive Departments and Agencies*, May 14, 1998, <http://www.cdt.org/privacy/survey/presmemo.html>.

⁵⁷⁵ William Matthews, "Privacy Czar Plays Homeland Role," *Federal Computer Week*, November 21, 2002, <http://www.fcw.com/fcw/articles/2002/1118/web-private-11-21-02.asp>.

⁵⁷⁶ U.S. House, Committee on the Judiciary, Subcommittee on Commercial and Administrative Law, *Privacy in the Hands of the Government: The Privacy Officer for the Department of Homeland Security*, February 10, 2004.

- Properly assessing the impact of its practices and rules on privacy.⁵⁷⁷

The privacy office, however, is only responsible for evaluating the privacy of programs within DHS. Many of the technologies, information sharing, and gathering mechanisms relating to homeland security are being implemented by the Administration in agencies other than DHS. The result is that there is no comprehensive and uniform evaluation of homeland security privacy issues in the federal government, especially in light of the elimination of the privacy counselor position within the White House. Without a single, accountable senior official to ensure that homeland security programs are evaluated in a uniform manner, our nation's privacy and civil liberties are at risk.

SECURITY RECOMMENDATION

The Administration should move promptly to name a person responsible for government-wide leadership on privacy issues. The government should create a Chief Privacy Officer responsible for evaluating privacy-related issues that arise in the information age, including those relating to the Privacy Act and the use of new technologies and information sharing mechanisms. In addition, the Administration should consider creating offices similar to the DHS privacy office in other agencies that handle large amounts of sensitive information, including the Departments of Treasury, Health and Human Services, the Social Security Administration, and the Department of Justice.

⁵⁷⁷ Roy Mark, "Homeland Security Names First Privacy Czar," *dc.internet.com*, April 17, 2003, <http://dc.internet.com/news/article.php/2192521>.